(19)日本国特許庁（ＪＰ）

(12)公開特許公報(A)

(11)特許出願公開番号
特開2001－127785
(P2001－127785A)

(43)公開日　平成13年５月11日(2001.5.11)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
H04L	12/46		G06F	13/38	350	5B077
	12/28		H04L	11/00	310C	5J104
G06F	13/38	350		9/00	673B	5K030
H04L	9/32			11/00	320	5K032
	12/40			11/20	B	5K033

審査請求　未請求　請求項の数16　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願平11－310295

(22)出願日　平成11年10月29日(1999.10.29)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

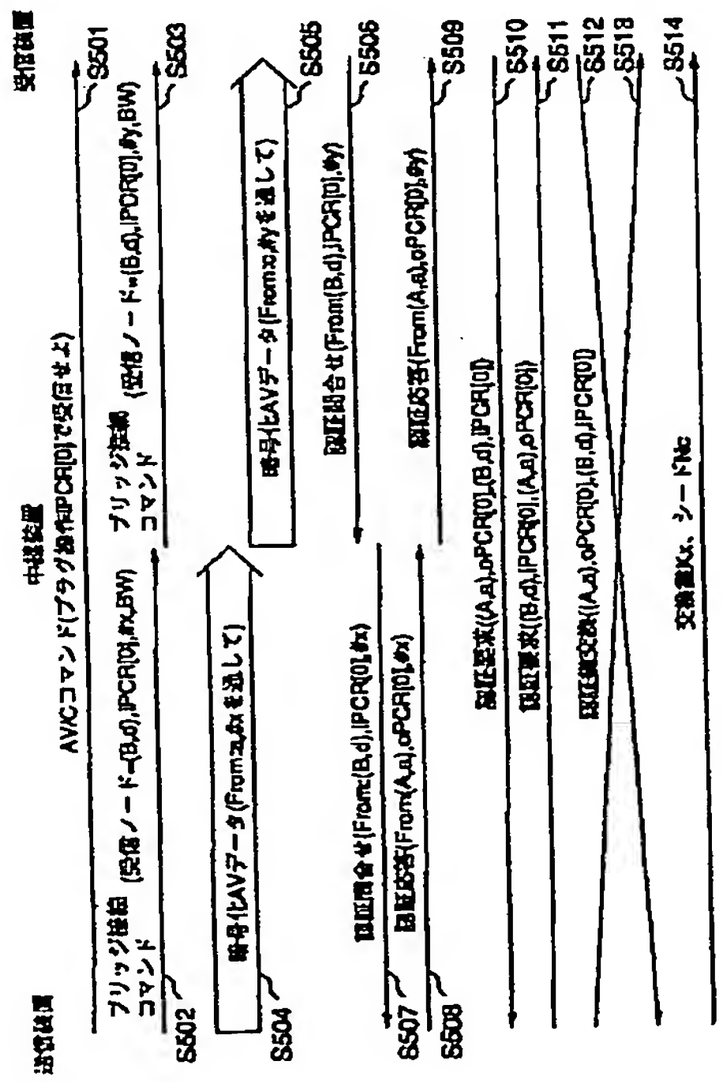
(72)発明者　高畠　由彰
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　ネットワーク接続装置、通信装置及びネットワーク接続方法

(57)【要約】
【課題】　同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とするネットワーク接続装置を提供すること。
【解決手段】　第１のＩＥＥＥ１３９４バス上の送信装置から、同期チャネル＃ｘ、ネットワーク接続装置、同期チャネル＃ｙの経路で、第２のＩＥＥＥ１３９４バス上の受信装置へ、暗号化されたデータが転送される。受信装置は、このデータが暗号化されている場合、ネットワーク接続装置にこのデータの送信装置に関する情報の問い合わせを行う。ネットワーク接続装置は、これに応答して、該データの送信装置に関する情報の問い合わせを第１のＩＥＥＥ１３９４バス上で行い、これによって得られた送信装置に関する情報を、受信装置に通知する。受信装置は、受信された前記情報に基づいて、送信装置との間で、直接認証・鍵交換手続きを行う。



【特許請求の範囲】
【請求項１】第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続装置において、
前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記第１のＩＥＥＥ１３９４バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、
前記データを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルまたは第２の非同期ストリームチャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送するデータ転送手段と、
前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、
前記問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに該情報の問い合わせを行う問い合わせ手段と、
前記送信ノードから、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、該情報の問い合わせに対する応答を受信する応答受信手段と、
前記応答を、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに通知する応答通知手段とを具備したことを特徴とするネットワーク接続装置。
【請求項２】前記所定のパケットは、同期パケット、非同期ストリーム、非同期パケットのいずれかであることを特徴とする請求項１に記載のネットワーク接続装置。
【請求項３】前記応答受信手段が受信する前記応答のパケットには、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれることを特徴とする請求項１に記載のネットワーク接続装置。
【請求項４】前記第２のＩＥＥＥ１３９４バス上の受信ノードは、通知を受けた前記情報に基づいて、前記第１のＩＥＥＥ１３９４バス上の送信ノードとの間で直接、認証・鍵交換手続きを行うものであることを特徴とする請求項２または３に記載のネットワーク接続装置。
【請求項５】第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続装置において、
前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記第１のＩＥＥＥ１３９４バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、
前記データを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルまたは第２の非同期ストリームチャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送するデータ転送手段と、
前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、
前記問い合わせを受信した場合に、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第１の同期チャネルのデータを受信するものであるとして、該情報の問い合わせを行う問い合わせ手段と、
前記送信ノードから、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、該情報の問い合わせに対する応答を受信する応答受信手段と、
前記問い合わせを受信した場合に、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第２の同期チャネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知する応答通知手段とを具備したことを特徴とするネットワーク接続装置。
【請求項６】前記所定のパケットは、同期パケット、非同期ストリーム、非同期パケットのいずれかであることを特徴とする請求項５に記載のネットワーク接続装置。
【請求項７】前記問い合わせ受信手段が受信する前記問い合わせのパケットには、前記受信ノードに関する情報として、前記受信ノードを識別する情報および前記データの転送のために用いられる前記受信ノードのプラグまたはサブユニットを識別する情報が含まれ、
前記応答受信手段が受信する前記応答のパケットには、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれ、
前記ネットワーク接続装置は、
前記第１のＩＥＥＥ１３９４バス上で前記問い合わせに応答した送信ノードのプラグまたはサブユニットと自装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第１の認証・鍵交換処理手段と、
自装置の仮想的なプラグまたはサブユニットと前記第２のＩＥＥＥ１３９４バス上の受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第２の認証・鍵交換処理手段とを更に具備したことを特徴とする請求項５に記載のネットワーク接続装置。
【請求項８】前記第１の認証・鍵交換処理手段による認証・鍵交換手続きが完了した後に、前記第１のＩＥＥＥ１３９４バス上の送信ノードから、前記仮想的なプラグまたはサブユニットに関係する暗号鍵に関する情報を受信する暗号鍵情報受信手段と、
前記第２の認証・鍵交換処理手段による認証・鍵交換手続きの少なくとも一部が完了した後に、前記暗号鍵に関する情報を、前記第２のＩＥＥＥ１３９４上の受信ノードに転送する暗号鍵情報転送手段とを更に具備したこと

を特徴とする請求項７に記載のネットワーク接続装置。
【請求項９】前記第１の同期チャネルまたは前記第１の非同期ストリームチャネルを識別する情報と、前記送信ノードを識別する情報と、前記第２の同期チャネルまたは前記第２の非同期ストリームチャネルを識別する情報との対応関係を記憶する記憶手段を更に具備し、
前記問い合わせ手段で受信した情報に含まれる前記第２の同期チャネルまたは前記第２の非同期ストリームチャネルを識別する情報に基づいて、前記記憶手段に記憶された前記対応関係を参照して決定した前記送信ノードに対して前記情報の問い合わせを行うことを特徴とする請求項１または５に記載のネットワーク接続装置。
【請求項１０】同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、１つ以上の暗号鍵を使用する第１のネットワークと、同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、同一の暗号鍵を使用し、かつ所定のチャネルを介してデータの送信及び又は受信を行う第２のネットワークとを接続するネットワーク接続装置において、
前記第１のネットワーク上に接続されたノードから転送されたデータを受信するデータ受信手段と、
前記データを前記第２のネットワーク上の所定のチャネルを介して、前記第２のネットワーク上に接続されたノードに転送するデータ転送手段と、
前記第２のネットワーク上に接続されたノードから、認証要求を受信する認証要求受信手段と、
前記認証要求を受信した場合に、前記第２のネットワーク上に接続されたノードに、該ノードが受信しているチャネルを識別する情報を問い合わせる問い合わせ手段と、
前記第２のネットワーク上に接続されたノードから、前記情報の問い合わせに対する応答を受信する応答受信手段と、
前記応答受信手段で受信した応答に含まれる情報により特定される前記第２のネットワーク上のチャネルに転送すべきデータを自装置に送信する前記第１のネットワーク上に接続されたノードから、該データのための暗号鍵に関する情報を受信する暗号鍵情報受信手段と、
前記暗号鍵に関する情報を、前記第２のネットワーク上のノードに転送する暗号鍵情報転送手段とを具備したことを特徴とするネットワーク接続装置。
【請求項１１】前記応答により特定される前記第２のネットワーク上のチャネルに転送すべきデータを自装置に送信する前記第１のネットワーク上に接続されたノードとの間で、認証・鍵交換手続きを行う第１の認証・鍵交換処理手段と、
前記応答により特定される前記第２のネットワーク上のチャネルを介して前記データを転送すべき前記第２のネットワーク上に接続されたノードとの間で認証・鍵交換手続きを行う第２の認証・鍵交換処理手段とを更に具備したことを特徴とする請求項１０に記載のネットワーク接続装置。
【請求項１２】第１のネットワークと第２のネットワークとを接続するネットワーク接続装置において、
自装置と前記第１のネットワーク上の任意の装置との間において、暗号管理情報が同一で且つ異なるフローに属するデータの暗号化は異なる暗号鍵で行い、
自装置と前記第２のネットワーク上の任意の装置との間において、暗号管理情報を同じくするデータの暗号化は同一の暗号鍵で行うことを特徴とするネットワーク接続装置。
【請求項１３】自装置と同一のＩＥＥＥ１３９４バスに接続されたネットワーク接続装置を介して他のＩＥＥＥ１３９４バス上の送信ノードからのデータを受信する通信装置において、
前記同一のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、
受信された前記データが暗号化されている場合に、前記同一のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、
前記問い合わせを受信した前記ネットワーク接続装置が前記他のＩＥＥＥ１３９４バス上で該情報の問い合わせを行って取得した該情報の問い合わせに対する応答を、前記同一のＩＥＥＥ１３９４バス上の所定のパケットを介して該ネットワーク接続装置から受信する応答受信手段と、
前記応答受信手段で受信した前記応答に含まれる情報に基づいて、前記他のＩＥＥＥ１３９４バス上の送信ノードとの間で直接、認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする通信装置。
【請求項１４】自装置と同一のＩＥＥＥ１３９４バスに接続されたネットワーク接続装置を介して他のＩＥＥＥ１３９４バス上の送信ノードからのデータを受信する通信装置において、
前記同一のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、
受信された前記データが暗号化されている場合に、前記同一のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、
前記問い合わせを受信した前記ネットワーク接続装置から、前記同一のＩＥＥＥ１３９４バス上の所定のパケッ

トを介して、該ネットワーク接続装置を送信ノードとする前記送信ノードに関する情報を含む、前記問い合わせに対する応答を受信する通知受信手段と、
前記通知受信手段で受信した前記通知に含まれる情報に基づいて、前記ネットワーク接続装置との間で認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする通信装置。
【請求項１５】第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続方法において、
前記第１のＩＥＥＥ１３９４バス上の送信ノードは、暗号化されたデータを前記第１の同期チャネルを介して送信し、
前記ネットワーク接続装置は、前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送し、
前記受信ノードは、前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、
前記ネットワーク接続装置は、前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに、該情報の問い合わせを行い、
前記送信ノードは、前記ネットワーク接続装置から、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記情報の問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該情報の問い合わせに対する応答を送信し、
前記ネットワーク接続装置は、前記送信ノードから、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記情報の問い合わせに対する応答を受信した場合、該応答を、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに通知し、
前記受信ノードは、前記通知に含まれる情報に基づいて、前記送信ノードとの間で、直接認証・鍵交換手続きを行うことを特徴とするネットワーク接続方法。
【請求項１６】第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続方法において、
前記第１のＩＥＥＥ１３９４バス上の送信ノードは、暗号化されたデータを前記第１の同期チャネルを介して送信し、
前記ネットワーク接続装置は、前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送し、
前記受信ノードは、前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、
前記ネットワーク接続装置は、前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受けた場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第１の同期チャネルのデータを受信するものであるとして、該情報の問い合わせを行うとともに、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第２の同期チャネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知し、
前記送信ノードは、前記ネットワーク接続装置から、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記情報の問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該送信ノードを識別する情報および前記暗号化されたデータの転送のために用いられる該送信ノードのプラグまたはサブユニットを識別する情報を含む、該情報の問い合わせに対する応答を送信し、
前記送信ノードのプラグまたはサブユニットと前記ネットワーク接続装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行うとともに、前記ネットワーク接続装置の仮想的なプラグまたはサブユニットと前記受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行うことを特徴とするネットワーク接続方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＥＥＥ１３９４バスや無線ネットワーク等のネットワーク間のデータ転送を中継するネットワーク接続装置及びネットワーク接

続方法、並びにＩＥＥＥ１３９４バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【０００２】

【従来の技術】近年、デジタル放送の開始や、デジタル機器の発売等、いわゆる「家庭ＡＶ環境のデジタル化」が大きな注目を集めている。デジタルＡＶデータは、様々な圧縮が可能、マルチメディアデータとしての処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【０００３】しかしながら、このデジタルＡＶ技術には、「コンテンツの不正コピーを行うことが比較的容易である」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビット」のコピーで、元通りの品質の、しかも未来永劫にわたって一切劣化の無い複製を作ることができてしまうため、いわゆる「不正コピー」の問題が発生する。

【０００４】この「不正コピー」を防ぐための技術がいくつか検討されている。その中の１つが、ＣＰＴＷＧ（コピープロテクション技術ワーキンググループ）で検討されている「１３９４ＣＰコンテンツ保護システム仕様（１３９４ＣＰ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ ＳｙｓｔｅｍＳｐｅｃｉｆｉｃａｔｉｏｎ）」である。この技術は、ＩＥＥＥ１３９４バスに接続されたノード間で、転送するコンテンツ（例えば、ＭＰＥＧデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外にはコンテンツが読めないようにする技術である。

【０００５】このようにすることにより、認証を行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【０００６】

【発明が解決しようとする課題】ＩＥＥＥ１３９４バスは、「最低速度でも１００Ｍｂｐｓ」、「網そのものに自動構成認識機能が備わっている」、「ＱＯＳ転送機能を持つ」等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルＡＶ向けのネットワークとして、デファクトスタンダードの地位を築いている。

【０００７】しかしながら、このようなＩＥＥＥ１３９４の特徴ゆえに、「ＩＥＥＥ１３９４と他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とＩＥＥＥ１３９４バスを接続する場合には、無線網や公衆網が１００Ｍｂｐｓ以上といった高速性を一般には有していないことや、ＩＥＥＥ１３９４の自動構成認識機能を無線網や公衆網へそのまま拡張するといった方法が簡単にはとれないことから、ＩＥＥＥ１３９４プロトコルをそのまま無線網や公衆網に拡張するといった方法を使うことはできない。

【０００８】そこで、ＩＥＥＥ１３９４と無線網や公衆網等の他網との間にプロトコル変換ゲートウェイを配置して相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等も提案されている。

【０００９】ところが、これらの方法を、前述した１３９４コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術が未だＩＥＥＥ１３９４バスについてのみ定められている状況である。このコピープロテクション技術を「ＩＥＥＥ１３９４と他のネットワークを接続するとき」に拡張するための技術は無いのが現状である。

【００１０】また、ＩＥＥＥ１３９４バス同士を接続する場合には、以下の問題点があった。

【００１１】ＩＥＥＥ１３９４バスに接続された送信ノードが、暗号化されたデータを送信する場合は、暗号化されたデータ、送信元のノードＩＤ、送信チャネルの少なくとも３つを含んだパケットを送信する。

【００１２】このデータをネットワーク接続装置を介して接続された他のＩＥＥＥ１３９４バスに接続された受信ノードに送信する場合、次の２つのケースが考えられる。第１のケースでは、ネットワーク接続装置は、このパケットの送信元を自装置のノードＩＤに書き換える。この場合、送信ノードと受信ノードが直接認証・鍵交換をすることはできないという問題があった。一方、第２のケースでは、ネットワーク接続装置が、送信元のノードＩＤを書き換えないでデータを転送する。この場合、異なるＩＥＥＥ１３９４バス上であるため、ノードＩＤの重複が発生し、正確なデータの転送がなされないという問題があった。

【００１３】従来のコピープロテクション技術は、ＩＥＥＥ１３９４同士を１３９４ブリッジで接続したシステムに拡張するには不十分であった。

【００１４】本発明は、上記事情を考慮してなされたもので、ＩＥＥＥ１３９４バス同士を接続する１３９４ブリッジで接続したネットワークあるいはＩＥＥＥ１３９４バス同士を他の無線ネットワークで接続するシステムにおいて、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とするネットワーク接続装置、通信装置及びネットワーク接続方法を提供することを目的とする。

【００１５】また、本発明は、コピープロテクション技

術をＩＥＥＥ１３９４のみならず、これと相互接続された他網にも拡張可能なネットワーク接続装置、通信装置及びネットワーク接続方法を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明（請求項１）は、第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続装置において、前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記第１のＩＥＥＥ１３９４バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、前記データを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルまたは第２の非同期ストリームチャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送するデータ転送手段と、前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、前記問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに該情報の問い合わせを行う問い合わせ手段と、前記送信ノードから、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、該情報の問い合わせに対する応答を受信する応答受信手段と、前記応答を、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに通知する応答通知手段とを具備したことを特徴とする。

【００１７】好ましくは、前記所定のパケットは、同期パケット、非同期ストリーム、非同期パケットのいずれかであるようにしてもよい。

【００１８】好ましくは、前記応答受信手段が受信する前記応答のパケットには、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれるようにしてもよい。

【００１９】好ましくは、前記第２のＩＥＥＥ１３９４バス上の受信ノードは、通知を受けた前記情報に基づいて、前記第１のＩＥＥＥ１３９４バス上の送信ノードとの間で直接、認証・鍵交換手続きを行うものであるようにしてもよい。

【００２０】好ましくは、前記第１の同期チャネルまたは前記第１の非同期ストリームチャネルを識別する情報と、前記送信ノードを識別する情報と、前記第２の同期チャネルまたは前記第２の非同期ストリームチャネルを識別する情報との対応関係を記憶する記憶手段を更に具備し、前記問い合わせ手段で受信した情報に含まれる前記第２の同期チャネルまたは前記第２の非同期ストリームチャネルを識別する情報に基づいて、前記記憶手段に記憶された前記対応関係を参照して決定した前記送信ノードに対して前記情報の問い合わせを行うようにしてもよい。

【００２１】また、本発明（請求項５）は、第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続装置において、前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記第１のＩＥＥＥ１３９４バス上に接続された送信ノードから転送されたデータを受信するデータ受信手段と、前記データを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルまたは第２の非同期ストリームチャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送するデータ転送手段と、前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受信する問い合わせ受信手段と、前記問い合わせを受信した場合に、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第１の同期チャネルのデータを受信するものであるとして、該情報の問い合わせを行う問い合わせ手段と、前記送信ノードから、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、該情報の問い合わせに対する応答を受信する応答受信手段と、前記問い合わせを受信した場合に、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに、自装置の仮想的なプラグまたはサブユニットが前記第２の同期チャネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知する応答通知手段とを具備したことを特徴とする。

【００２２】好ましくは、前記所定のパケットは、同期パケット、非同期ストリーム、非同期パケットのいずれかであるようにしてもよい。

【００２３】好ましくは、前記問い合わせ受信手段が受信する前記問い合わせのパケットには、前記受信ノードに関する情報として、前記受信ノードを識別する情報および前記データの転送のために用いられる前記受信ノードのプラグまたはサブユニットを識別する情報が含まれ、前記応答受信手段が受信する前記応答のパケットには、前記送信ノードに関する情報として、前記送信ノードを識別する情報および前記データの転送のために用いられる前記送信ノードのプラグまたはサブユニットを識別する情報が含まれ、前記ネットワーク接続装置は、前記第１のＩＥＥＥ１３９４バス上で前記問い合わせに応答した送信ノードのプラグまたはサブユニットと自装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第１の認証・鍵交換処理手段と、自装置の仮想的なプラグまたはサブユニットと前記第２のＩＥＥＥ１３９４バス上の受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行う第２の認証

・鍵交換処理手段とを更に具備するようにしてもよい。
【００２４】好ましくは、前記第１の認証・鍵交換処理手段による認証・鍵交換手続きが完了した後に、前記第１のＩＥＥＥ１３９４バス上の送信ノードから、前記仮想的なプラグまたはサブユニットに関係する暗号鍵に関する情報を受信する暗号鍵情報受信手段と、前記第２の認証・鍵交換処理手段による認証・鍵交換手続きの少なくとも一部が完了した後に、前記暗号鍵に関する情報を、前記第２のＩＥＥＥ１３９４上の受信ノードに転送する暗号鍵情報転送手段とを更に具備するようにしてもよい。
【００２５】好ましくは、前記第１の同期チャネルまたは前記第１の非同期ストリームチャネルを識別する情報と、前記送信ノードを識別する情報と、前記第２の同期チャネルまたは前記第２の非同期ストリームチャネルを識別する情報との対応関係を記憶する記憶手段を更に具備し、前記問い合わせ手段で受信した情報に含まれる前記第２の同期チャネルまたは前記第２の非同期ストリームチャネルを識別する情報に基づいて、前記記憶手段に記憶された前記対応関係を参照して決定した前記送信ノードに対して前記情報の問い合わせを行うようにしてもよい。
【００２６】また、本発明（請求項１０）は、同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、１つ以上の暗号鍵を使用する第１のネットワークと、同一ネットワークに接続されているノード間での暗号化データの送信及び又は受信においては、同一の暗号鍵を使用し、かつ所定のチャネルを介してデータの送信及び又は受信を行う第２のネットワークとを接続するネットワーク接続装置において、前記第１のネットワーク上に接続されたノードから転送されたデータを受信するデータ受信手段と、前記データを前記第２のネットワーク上の所定のチャネルを介して、前記第２のネットワーク上に接続されたノードに転送するデータ転送手段と、前記第２のネットワーク上に接続されたノードから、認証要求を受信する認証要求受信手段と、前記認証要求を受信した場合に、前記第２のネットワーク上に接続されたノードに、該ノードが受信しているチャネルを識別する情報を問い合わせる問い合わせ手段と、前記第２のネットワーク上に接続されたノードから、前記情報の問い合わせに対する応答を受信する応答受信手段と、前記応答受信手段で受信した応答に含まれる情報により特定される前記第２のネットワーク上のチャネルに転送すべきデータを自装置に送信する前記第１のネットワーク上に接続されたノードから、該データのための暗号鍵に関する情報を受信する暗号鍵情報受信手段と、前記暗号鍵に関する情報を、前記第２のネットワーク上のノードに転送する暗号鍵情報転送手段とを具備したことを特徴とする。
【００２７】好ましくは、前記応答により特定される前記第２のネットワーク上のチャネルに転送すべきデータを自装置に送信する前記第１のネットワーク上に接続されたノードとの間で、認証・鍵交換手続きを行う第１の認証・鍵交換処理手段と、前記応答により特定される前記第２のネットワーク上のチャネルを介して前記データを転送すべき前記第２のネットワーク上に接続されたノードとの間で認証・鍵交換手続きを行う第２の認証・鍵交換処理手段とを更に具備するようにしてもよい。
【００２８】また、本発明（請求項１２）は、第１のネットワークと第２のネットワークとを接続するネットワーク接続装置において、自装置と前記第１のネットワーク上の任意の装置との間において、暗号管理情報が同一で且つ異なるフローに属するデータの暗号化は異なる暗号鍵で行い、自装置と前記第２のネットワーク上の任意の装置との間において、暗号管理情報を同じくするデータの暗号化は同一の暗号鍵で行うことを特徴とする。暗号管理情報は、例えば、「このデータは何回コピー可」、「このデータはコピー不可」等、送られるデータのコピーをどの様に扱うかが記載されている情報である。
【００２９】また、本発明（請求項１３）は、自装置と同一のＩＥＥＥ１３９４バスに接続されたネットワーク接続装置を介して他のＩＥＥＥ１３９４バス上の送信ノードからのデータを受信する通信装置において、前記同一のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、受信された前記データが暗号化されている場合に、前記同一のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、前記問い合わせを受信した前記ネットワーク接続装置が前記他のＩＥＥＥ１３９４バス上で該情報の問い合わせを行って取得した該情報の問い合わせに対する応答を、前記同一のＩＥＥＥ１３９４バス上の所定のパケットを介して該ネットワーク接続装置から受信する応答受信手段と、前記応答受信手段で受信した前記応答に含まれる情報に基づいて、前記他のＩＥＥＥ１３９４バス上の送信ノードとの間で直接、認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする。
【００３０】また、本発明（請求項１４）は、自装置と同一のＩＥＥＥ１３９４バスに接続されたネットワーク接続装置を介して他のＩＥＥＥ１３９４バス上の送信ノードからのデータを受信する通信装置において、前記同一のＩＥＥＥ１３９４バス上の第１の同期チャネルまたは第１の非同期ストリームチャネルを介して、前記ネットワーク接続装置から転送されたデータを受信するデータ受信手段と、受信された前記データが暗号化されている場合に、前記同一のＩＥＥＥ１３９４バス上の所定の

パケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行う問い合わせ手段と、前記問い合わせを受信した前記ネットワーク接続装置から、前記同一のＩＥＥＥ１３９４バス上の所定のパケットを介して、該ネットワーク接続装置を送信ノードとする前記送信ノードに関する情報を含む、前記問い合わせに対する応答を受信する通知受信手段と、前記通知受信手段で受信した前記通知に含まれる情報に基づいて、前記ネットワーク接続装置との間で認証・鍵交換手続きを行う認証・鍵交換処理手段とを備えたことを特徴とする。

【００３１】また、本発明（請求項１５）は、第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続方法において、前記第１のＩＥＥＥ１３９４バス上の送信ノードは、暗号化されたデータを前記第１の同期チャネルを介して送信し、前記ネットワーク接続装置は、前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送し、前記受信ノードは、前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、前記ネットワーク接続装置は、前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに、該情報の問い合わせを行い、前記送信ノードは、前記ネットワーク接続装置から、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記情報の問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該情報の問い合わせに対する応答を送信し、前記ネットワーク接続装置は、前記送信ノードから、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記情報の問い合わせに対する応答を受信した場合、該応答を、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに通知し、前記受信ノードは、前記通知に含まれる情報に基づいて、前記送信ノードとの間で、直接認証・鍵交換手続きを行うことを特徴とする。

【００３２】また、本発明（請求項１６）は、第１のＩＥＥＥ１３９４バスと第２のＩＥＥＥ１３９４バスとを接続するネットワーク接続方法において、前記第１のＩＥＥＥ１３９４バス上の送信ノードは、暗号化されたデータを前記第１の同期チャネルを介して送信し、前記ネットワーク接続装置は、前記第１のＩＥＥＥ１３９４バス上の第１の同期チャネルを介して、前記送信ノードから転送されてきた前記暗号化されたデータを受信し、このデータを前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して、前記第２のＩＥＥＥ１３９４バス上に接続された受信ノードに転送し、前記受信ノードは、前記第２のＩＥＥＥ１３９４バス上の第２の同期チャネルを介して転送されてきたデータを受信し、該データが暗号化されたものである場合、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該受信ノードを識別する情報および該暗号化されたデータの転送のために用いられる該受信ノードのプラグまたはサブユニットを識別する情報を含む、該暗号化されたデータの送信ノードに関する情報の問い合わせを行い、前記ネットワーク接続装置は、前記受信ノードから、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに関する情報の問い合わせを受けた場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記送信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第１の同期チャネルのデータを受信するものであるとして、該情報の問い合わせを行うとともに、前記第２のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記受信ノードに、該ネットワーク接続装置の仮想的なプラグまたはサブユニットが前記第２の同期チャネルのデータを送信するものであるとして、該情報の問い合わせに対する応答を通知し、前記送信ノードは、前記ネットワーク接続装置から、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記情報の問い合わせを受信した場合、前記第１のＩＥＥＥ１３９４バス上の所定のパケットを介して、前記ネットワーク接続装置に、該送信ノードを識別する情報および前記暗号化されたデータの転送のために用いられる該送信ノードのプラグまたはサブユニットを識別する情報を含む、該情報の問い合わせに対する応答を送信し、前記送信ノードのプラグまたはサブユニットと前記ネットワーク接続装置の仮想的なプラグまたはサブユニットとの間で認証・鍵交換手続きを行うとともに、前記ネットワーク接続装置の仮想的なプラグまたはサブユニットと前記受信ノードのプラグまたはサブユニットとの間で認証・鍵交換手続きを行うことを特徴とする。

【００３３】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００３４】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記

録したコンピュータ読取り可能な記録媒体としても成立する。

【００３５】本発明（請求項１等）によれば、ネットワーク接続装置が、第２のＩＥＥＥ１３９４バス上の受信ノードに、第１のＩＥＥＥ１３９４バス上の送信ノードに関する情報を通知してあげるので、受信ノードはネットワークの異なる送信ノードとの間で直接、認証・鍵交換手続きを行うことができ、同じネットワークには接続されていない送受信ノード間のコンテンツ保護手続きが可能となる。

【００３６】また、本発明（請求項５等）によれば、認証問い合わせ手続きにおいて、ネットワーク接続装置が、第１のＩＥＥＥ１３９４バス上の送信ノード／第２のＩＥＥＥ１３９４バス上の受信ノードにそれぞれ自装置を受信ノード／送信ノードとして通知し、認証・鍵交換手続きについて、ネットワーク接続装置が、第１のＩＥＥＥ１３９４バス上の送信ノードとの間および第２のＩＥＥＥ１３９４バス上の受信ノードとの間でそれぞれ行い、鍵に関する情報については、送信ノードから受信ノードにフォワードするので、同じネットワークには接続されていない送受信ノード間のコンテンツ保護手続きが可能となる。

【００３７】また、本発明（請求項１０等）によれば、ネットワーク接続装置は、第２のネットワーク上の受信ノードから認証要求を受信した場合に、該受信ノードが受信している同期チャネルを確認し、その同期チャネルに転送すべきデータを第１のネットワーク上で送信するノードから該データのための暗号鍵に関する情報を通知された場合、これを第２のネットワーク上の受信ノードに通知するので、同じネットワークには接続されていない送受信ノード間のコンテンツ保護手続きが可能となる。

【００３８】また、本発明では、ネットワーク接続装置は暗号化されたデータを復号化することなくフォワードすることができるため、ネットワーク接続装置を通過する毎に暗号の復号化および再暗号化を行う必要がなくなり、大幅な処理コストの低減を図ることができる。

【００３９】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００４０】（第１の実施形態）図１に、本発明を適用するネットワークの全体構成の一例を示す。

【００４１】本実施形態においては図１のネットワークに例示するように、２つのＩＥＥＥ１３９４バス１０４，１０５が中継装置（もしくはネットワーク中継装置）１０２によりブリッジ接続されているネットワークにおいて、第１のＩＥＥＥ１３９４バス（１０４）に接続された送信装置１０１から中継装置１０２を介して第２のＩＥＥＥ１３９４バス（１０５）に接続された受信装置１０３に対して、ＡＶストリームを転送する場合を例にとって説明する。その際に、その著作権保護（不正コピーの防止）のために、送信ノード（１０１）と受信ノード（１０３）との間で転送されるＡＶストリームは暗号化される場合を考える。また、上記ＡＶストリームの一例としてＭＰＥＧ映像データを用いて説明する。

【００４２】本実施形態では、ＩＥＥＥ１３９４バス上での認証・鍵交換は、ＡＶデータフロー毎あるいはＡＶ／Ｃのプラグ毎に行われ、同じノード間でフロー毎あるいはプラグ毎に異なる暗号鍵Ｋを使用することが可能であるものとする。ここで、ＰＣＲ（プラグコントロールレジスタ、ｉＰＣＲ（入力プラグコントロールレジスタ）やｏＰＣＲ（出力プラグコントロールレジスタ））は、ＩＥＥＥ１３９４ＡＶ／Ｃスペックにて規定される論理的な番号であり、ネットワークインタフェース（本実施形態の場合、ＩＥＥＥ１３９４Ｉ／Ｆ）から入力または出力されるＡＶストリームデータを入力または出力する入口番号または出口番号と考えればよい。なお、以下で使う具体的なＰＣＲの番号は一例である。

【００４３】第１のＩＥＥＥ１３９４バス（１０４）のバスＩＤを“Ａ”、第２のＩＥＥＥ１３９４バス（１０５）のバスＩＤを“Ｂ”とする。送信装置１０１の物理ＩＤを“ａ”、受信装置１０３の物理ＩＤを“ｄ”とする。ノードのノードＩＤ（アドレス）は、（バスＩＤ、物理ＩＤ）で定義される。送信装置１０１のノードＩＤは（Ａ，ａ）、受信装置１０３のノードＩＤは（Ｂ，ｄ）で表される。中継装置１０２の第１のＩＥＥＥ１３９４（１０４）側のインタフェースのノードＩＤを（Ａ，ｂ）、中継装置１０２の第２のＩＥＥＥ１３９４（１０５）側のインタフェースのノードＩＤを（Ｂ，ｃ）とする。

【００４４】なお、本実施形態では、本例において送信側となるノードを送信装置、本例において受信側となるノードを受信装置と呼んでいるが、もちろん、送信装置１０１や受信装置１０３は、後述する送信側としての機能や受信側としての機能以外の機能を持っていても良いし（送信側としての機能と受信側としての機能の両方の機能を持っていても良い）、また、図１では、３つのノード１０１，１０２，１０３のみを示してあるが、これらの他にもノードが接続されていてももちろんよい（この点は、後述する他の実施形態においても同様である）。

【００４５】図２に、送信装置１０１の内部構成例を示す。

【００４６】送信装置１０１は、図２に示されるように、ＩＥＥＥ１３９４インタフェース２０１、ＡＶ／Ｃ（ＡＶ／Ｃ Ｄｉｇｉｔａｌ Ｉｎｔｅｒｆａｃｅ Ｃｏｍｍａｎｄ Ｓｅｔ Ｇｅｎｅｒａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ）プロトコルの処理を行う、ＡＶ／Ｃプロトコル処理部２０２、ＡＶ／Ｃプロトコル内のコピープロテクションに関する処理を行う、コピープロテクシ

ョン処理部２０３、ＩＥＥＥ１３９４を通して送受信されるデータのうち同期チャネルを通してやり取りされるデータについて送受信する、ＩＳＯ信号送受信部２０４、ＭＰＥＧ映像のストレージである、ＭＰＥＧストレージ部２０６、コピープロテクション処理部２０３から暗号鍵Ｋを貰いＭＰＥＧ映像を暗号化してＩＳＯ信号送受信部２０４に送出する、暗号化部２０５を有する。

【００４７】送信装置１０１は、ＭＰＥＧ映像データを蓄積可能なノードであり、要求に応じてＭＰＥＧ映像データを送出する。その際、転送経路上で不法にコピーをされることを未然に防止するために必要な場合には送出するＭＰＥＧ映像データを暗号化して送出する機能を持つ。そのため、自装置が送出するＭＰＥＧ映像データを受信するノードとの間で認証データや暗号鍵等の交換を行うための機構も持つ。

【００４８】本例では、送信装置１０１は、受信装置１０３との間でＡＶストリームのやり取りを暗号化を施した上で行うために直接的には中継装置１０２との間で、間接的に受信装置１０３との間で、認証・鍵交換手続きを行う。このための認証・鍵交換手続きを行うのが認証のための機器証明（認証フォーマット）Ａｃｅｒｔを内部に持つコピープロテクション処理部２０３である。

【００４９】ＩＥＥＥ１３９４の場合は、認証・鍵交換の手続きはＡＶ／Ｃプロトコルに含まれるため、ＡＶ／Ｃプロトコル処理部２０２にて多重化処理が行われ、ＩＥＥＥ１３９４インタフェース（Ｉ／Ｆ）２０１を通してパケットのやり取りがなされる。コピープロテクション処理部２０３にて、使用する暗号鍵Ｋが決まる。

【００５０】ここでは、送信装置１０１から送出されるＡＶストリームが、ＭＰＥＧストリームであるとする。ＭＰＥＧストレージ部２０６から送出されたＭＰＥＧストリームは、暗号化部２０５で暗号鍵Ｋにて暗号化され、ＩＳＯ信号送受信部２０４でＩＥＥＥ１３９４向けのパケット化やタイムスタンプ処理などがなされ、ＩＥＥＥ１３９４インタフェース２０１を通して第１のＩＥＥＥ１３９４バス（１０４）に対して送出される。

【００５１】図３に、受信装置１０３の内部構成例を示す。

【００５２】受信装置１０３は、図３に示されるように、ＩＥＥＥ１３９４インタフェース３０１、ＡＶ／Ｃプロトコルの処理を行う、ＡＶ／Ｃプロトコル処理部３０２、ＡＶ／Ｃプロトコル内のコピープロテクションに関する処理を行う、コピープロテクション処理部３０３、ＩＥＥＥ１３９４を通して送受信されるデータのうち同期チャネルを通してやり取りされるデータについて送受信する、ＩＳＯ信号送受信部３０４、受信した暗号化されたストリーム（ＭＰＥＧ映像等）をコピープロテクション処理部３０３から渡される暗号鍵Ｋを使ってこれを復号化する、暗号復号化部３０５、ＭＰＥＧデコード部３０６、映像を表示する、ディスプレイ部３０７を有する。

【００５３】受信装置１０３は、受信したＭＰＥＧ映像データをデコードし表示する機能を有する装置である。その際、転送経路上で不法にコピーをされることを未然に防止するために送信側が暗号化して送出したＭＰＥＧ映像データを復号化する機能を持つ。そのため、ＭＰＥＧ映像データを送信するノードとの間で認証データや暗号鍵等の交換を行うための機構も持つ。

【００５４】本例では、受信装置１０３は、送信装置１０１との間でＡＶストリームのやり取りを暗号化を施した上で行うために直接的には中継装置１０２との間で、間接的に送信装置１０１との間で、認証・鍵交換手続きを行う。このための認証・鍵交換手続きを行うのが認証のための機器証明Ｂｃｅｒｔを内部に持つコピープロテクション処理部３０３である。なお、機器証明Ｂｃｅｒｔの発行機関は、送信装置１０１の機器証明Ａｃｅｒｔの発行機関と同一の発行機関であるものとする。

【００５５】ＩＥＥＥ１３９４インタフェース（Ｉ／Ｆ）３０１を通してパケットを受信すると、コピープロテクションのための認証・鍵交換のためのパケットは、ＡＶ／Ｃプロトコル処理部３０２にて分離処理が行われ、コピープロテクション処理部３０３に渡される。この認証・鍵交換の手続きにより、ＡＶストリームの暗号化に使用される暗号鍵Ｋが決まる。

【００５６】ＩＥＥＥ１３９４インタフェース３０１を通して暗号化されたＡＶストリームを受信すると、ＩＳＯ信号送受信部３０４にて１３９４ヘッダの除去やタイムスタンプを用いた同期処理等が行われ、暗号化ＡＶストリームが暗号復号化部３０５に渡される。コピープロテクション処理部３０３から暗号鍵Ｋを貰い、これを復号して、ＭＰＥＧデコード部３０６でデコードし、これをディスプレイ部３０７で映像・音声として表示する。

【００５７】図４に、中継装置１０２の内部構成例を示す。

【００５８】中継装置１０２は、図４に示されるように、第１のＩＥＥＥ１３９４インタフェース（Ｉ／Ｆ）４０１、第２のＩＥＥＥ１３９４インタフェース（Ｉ／Ｆ）４０８、第１のＡＶ／Ｃプロトコル処理部４０２、第２のＡＶ／Ｃプロトコル処理部４０９、第１のコピープロテクション処理部４０３、第２のコピープロテクション処理部４１０、ブリッジテーブル部４０５、第１のＩＳＯ信号送受信部４０４、第２のＩＳＯ信号送受信部４０７、ブリッジ接続処理部４０６を有する。

【００５９】第１のコピープロテクション処理部４０３は、第１のＩＥＥＥ１３９４バス（１０４）上の装置（本例の場合、送信装置１０１）と認証・鍵交換手続きを行う。同様に、第２のコピープロテクション部４１０は、第２のＩＥＥＥ１３９４バス（１０５）上の装置（本例の場合、受信装置１０３）と認証・鍵交換手続きを行う。

【0060】IEEE1394のブリッジ接続においては、複数のIEEE1394バス間の同期チャネルを接続することが可能となる。この対応関係を記憶するのが、ブリッジテーブル部405である。

【0061】図5に、ブリッジテーブル部405が管理するブリッジテーブルの構成例を示す。ブリッジテーブルには、この例では、第1のIEEE1394バス(104)上の特定の同期チャネル(例えば、#x)と第2のIEEE1394バス(105)上の特定の同期チャネル(例えば、#y)との間の関係、すなわち、同期チャネル番号、どちらが送信側でどちらが受信側かを示す情報(送受信の方向)、送信者のノードID=(バスID、物理ID)、それぞれのチャネルに関して認証・鍵交換を行う認証先等が登録される。後述するように、これらの登録は順次行われていく。

【0062】次に、実際のコピープロテクションを施した上でのMPEG映像転送のための全体的なシーケンスについて、図6(全体のシーケンス例)、図7(中継装置102のフローチャート例)を参照しながら説明する。

【0063】まず、送信装置101が、受信装置103に対してAV/Cコマンドを発行し、そのプラグの操作を行う(S501)。具体的には、受信装置103の入力プラグコントロールレジスタ(iPCR)を操作し、例えば、「iPCR[0]を通してデータを受信する旨の要求」あるいは「ディスプレイサブユニットに対する映像表示要求」などのコマンドを発行する。なお、サブユニットは、AV/Cプロトコルにて規定されるノード内の機能要素である。

【0064】次に、送信装置101は、自装置から受信装置103に至る同期チャネルの確立を行うため、ブリッジ接続コマンドを発行する(S502)。

【0065】このブリッジ接続コマンドは、例えば「受信ノード(B, d)のiPCR[0]に至る同期チャネルを確立せよ。帯域はBW、第1のIEEE1394バス上の同期チャネル番号は#xを使用すること。」という内容を要求する情報を含む。このコマンドは、非同期パケットの形(例えば、受信装置103宛または中継装置102宛であり、さらにその特定のレジスタ宛になっていてもよい)で送信されても、非同期ストリームの形で送信されてもよいが、どちらの場合も中継装置102により一旦受信される。

【0066】なお、第1のIEEE1394バス(104)上に、中継装置102以外の中継装置が接続されていても、あるいはこのコマンドが受信されてもよいが、受信装置103に至る経路以外の中継装置は、このコマンドの処理は行わないものとする。

【0067】送信装置101から送信されたブリッジ接続コマンドは、中継装置102により受信(S701)される(そのブリッジ接続処理部406に渡される)。

【0068】このブリッジ接続コマンドを受信した中継装置102は、受信ノード(B, d)に至る経路上に自分がいることを認識すると、受信装置103に至る経路(第2のIEEE1394バス)の必要帯域BWをもった同期チャネル(#y)を確保し、ブリッジ接続コマンドを発行する(S503, S702, S704)。このブリッジ接続コマンドは、受信装置103宛の非同期パケットでもよい。このコマンドの中身は、記録されている同期チャネル番号が第2のIEEE1394バス上で使用される#yに書き換えられている以外は、S502におけるブリッジ接続コマンドとほぼ同様である。

【0069】上記コマンドの発行とともに(同時にもしくは相前後して)、ブリッジ接続処理部406は、図5のブリッジテーブルの「同期チャネル番号」の行と「送受信の方向」の行の値の設定を行う(S703)。このときのブリッジテーブルの登録内容が図5(a)である。

【0070】これらブリッジ接続コマンドにより、送信装置101と受信装置103との間の同期チャネルの経路(#x→#y)が確立される。

【0071】次に、送信装置101は、同期チャネル#xを通して、暗号鍵Kにて暗号化されたAVストリームを送信する(S504)。

【0072】なお、この時点ではまだ認証要求も認証・鍵交換も行われていない。また、受信装置103はまだ暗号鍵Kを得ていない。

【0073】中継装置102は、同期チャネル#xから上記暗号化AVストリームを受信(S705)すると、ブリッジテーブルを参照して、このAVストリームは第2のIEEE1394バス(105)側に同期チャネル#yで送信すべきものであると判断し、第2のIEEE1394バス(105)上の同期チャネル#yを通して、タイムスタンプの値などを適当に変更した上で、送信する(S505、S706)。このとき、暗号化されたAVストリームはそのまま送信する。

【0074】また、これとともに(同時にもしくは相前後して)、第1のIEEE1394バス(104)から受信された同期パケットの送信ノードIDを参照して、送信者のノードIDが(A, a)であることを認識すると、このID情報をブリッジテーブルの第1のIEEE1394バス側の送信者の欄に登録する(S705)。また、第2のIEEE1394バス側の送信者の欄は自分自身である。このときのブリッジテーブルの登録内容が図5(b)である。

【0075】次に、受信装置103は、同期チャネル#yを通して、上記暗号化AVストリームを受信する。ここで、受信装置103は、受信したデータが暗号化されていることを認識し、この暗号化データの送信者との間での認証・鍵交換の必要性を認識する。ここでは、認証・鍵交換のためには、まず、この暗号化データの送信者

（に関する情報）を取得するための手順を行う必要がある。
【００７６】そこで、受信装置１０３は、受信した暗号化データの送信者（に関する情報）を取得するために、認証問い合わせパケットを中継装置１０２に対して送信する（Ｓ５０６）。
【００７７】この認証問い合わせパケットは、第２のＩＥＥＥ１３９４バス（１０５）上の同期チャネル＃ｙに対してデータを送信しているのがどのノード（あるいはどのノードのどのプラグ）であるのかを確認するためのパケットである。また、このパケットには、この暗号化ＡＶデータを受信しているのが、受信装置１０３であることを示すために、同期チャネル番号＃ｙの他に、受信装置１０３のノードＩＤ（Ｂ，ｄ）と、受信しているプラグであるｉＰＣＲ［０］の値等も入っている。
【００７８】なお、実際には、この認証問い合わせパケットは、非同期ストリームにて送られるパケットでもよいが、暗号化ＡＶデータの送信ノードＩＤの値を見て、暗号化ＡＶデータを同期チャネル＃ｙにて送信しているのが中継装置１０２であることがわかるため、中継装置１０２宛の非同期パケットでもよい。
【００７９】この認証問い合わせパケットを受信（Ｓ７０７）した中継装置１０２は、ブリッジテーブルの認証先の欄に、「同期チャネル＃ｙを受信しているのは（Ｂ，ｄ）のｉＰＣＲ［０］である」旨を登録する（Ｓ７０８）。このときのブリッジテーブルの登録内容が図５（ｃ）である。
【００８０】さらに、この同期チャネルを送信しているのが第１のＩＥＥＥ１３９４バス上（１０４）の（Ａ，ａ）であることをブリッジテーブルを参照することにより確認（Ｓ７０８）し、（Ａ，ａ）に対して認証問い合わせをフォワードする（Ｓ５０７，Ｓ７０９）。その際は、認証問い合わせパケットにおける同期チャネル番号は、ブリッジテーブルを参照して、第１のＩＥＥＥ１３９４バス（１０４）上の同期チャネルに相当する＃ｘに変更しておく。
【００８１】この認証問い合わせパケットを受信した送信装置１０１は、同期チャネル＃ｘに対して送信しているのは、ノードＩＤが（Ａ，ａ）、プラグがｏＰＣＲ［０］である旨を、認証応答として返答する（Ｓ５０８）。このとき、認証応答の送信先は、Ｓ５０７における認証問い合わせの送信者であった中継装置１０２である。
【００８２】この認証応答を受信（Ｓ７１０）した中継装置１０２は、このパケットを参照して、ブリッジテーブルの第１のＩＥＥＥ１３９４側の認証先（（Ａ，ａ）、ｏＰＣＲ［０］）を登録する（Ｓ７１０）。このときのブリッジテーブルの登録内容が図５（ｄ）である。
【００８３】さらに、第２のＩＥＥＥ１３９４バス（１０５）上で使用している同期チャネル番号＃ｙに変更した上で受信装置１０３に認証応答をフォワードする（Ｓ５０９，Ｓ７１１）。
【００８４】以上の手続きにより、受信装置１０３は、認証・鍵交換を行うべき相手が、送信装置１０１（ノードＩＤが（Ａ，ａ）、プラグがｏＰＣＲ［０］）であることを認識する。この時点で、受信者である受信装置１０３は送信者である送信装置１０１と認証・鍵交換の手続きを行うことができるようになる。
【００８５】続いて、受信装置１０３は、認証要求を送信装置１０１に対して直接送信する（Ｓ５１０）。この認証要求には、送信側の装置のノードＩＤ（Ａ，ａ）とプラグｏＰＣＲ［０］、および受信側の装置のノードＩＤ（Ｂ，ｄ）とプラグｉＰＣＲ［０］の値が含まれていてもよい。また、この認証要求には受信装置の機器証明Ｂｃｅｒｔが含まれていてもよい。また、送信装置１０１も、認証要求を受信装置１０３に対して直接送信する（Ｓ５１１）。この認証要求にも、送受信側の装置のノードＩＤとプラグの値が含まれていてもよい。また、この認証要求には送信装置の機器証明Ａｃｅｒｔが含まれていてもよい。
【００８６】認証が成立すると、続いて、認証・鍵交換が行われ（Ｓ５１２，Ｓ５１３，Ｓ７１２）、送信装置１０１と受信装置１０３との双方で認証鍵が共有される。次に、送信装置１０１から受信装置１０２に対して、暗号鍵Ｋを計算するための交換鍵Ｋｘとシードｎｃが送信され（Ｓ５１４）、受信装置１０３は、交換鍵Ｋｘとシードｎｃをもとに暗号鍵Ｋを計算することができるようになる。
【００８７】これ以降、中継装置１０２を介して、送信装置１０１と受信装置１０３との間で暗号鍵Ｋによる暗号通信を行うことができる。
【００８８】すなわち、送信装置１０１が、送信するＭＰＥＧ映像を、暗号鍵Ｋを使って、暗号化部２０５にて暗号化し、これを第１の１３９４バス（１０４）の同期チャネル＃ｘを通して中継装置１０２に対して送信する。
【００８９】中継装置１０２は、送信装置１０１から同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、ＩＳＯ信号送受信部４０４から無線ＩＳＯ信号送受信部４０５を通して、無線同期チャネル＃ｙに送信する。
【００９０】これを受信した受信装置１０３は、暗号鍵Ｋの値を使ってＭＰＥＧ映像の値を復号化する。（暗号が）復号化されたＭＰＥＧデータは、ＭＰＥＧデコード部３０６にて（ＭＰＥＧ符号が）デコードされる。デコードされたデータは、例えば、ディスプレイ部３０７にて再生表示される。
【００９１】このように、あるＩＥＥＥ１３９４バスと他のＩＥＥＥ１３９４バスとの間にブリッジ・ノードが

存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信装置１０１と受信装置１０３）が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継装置１０２を含め、その他のノードが知ることはできない仕組みとなっている。また、コンテンツ保護を必要とする実際のＭＰＥＧ映像等のデータの転送も、コピーが不可能なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【００９２】なお、認証問い合わせパケットは、ＩＥＥＥ１３９４のＣＳＲ（コマンドステータスレジスタ）空間の特定のアドレス（レジスタ）に、その送信先を指定してもよいし、ＡＶ／Ｃのセキュリティコマンドの１つとしてこれを定義してもよい。

【００９３】本実施形態においては、ＰＣＲ（プラグコントロールレジスタ）番号を認証問い合わせに用いることによる例を示したが、ＰＣＲの代わりに、サブユニット番号や、ＡＶデータを転送している同期チャネル番号を用いて、認証問い合わせを行うように構成することも可能である。

【００９４】（第２の実施形態）次に、第２の実施形態について説明する。

【００９５】本実施形態も、第１の実施形態と同様に、ブリッジ接続されている場合の認証・鍵交換・暗号化データのやり取りについて説明するが、第１の実施形態との相違点は、中継装置も機器証明を持っており、第１のＩＥＥＥ１３９４バス上での認証・鍵交換と第２のＩＥＥＥ１３９４バス上での認証・鍵交換とをそれぞれ中継装置が終端する点である。ただし、暗号化データ、交換鍵Ｋｘの値、シードＮｃの値は中継装置では終端されずそのままフォワードされる。

【００９６】以下では、第１の実施形態と相違する点を中心に説明する。

【００９７】本実施形態のネットワーク構成例は図１と同様である。送信装置１０１の内部構成例は図２と同様である。受信装置１０３の内部構成例は図３と同様である。

【００９８】図８に、本実施形態の中継装置（もしくはネットワーク中継装置）１０２の内部構成例を示す。

【００９９】本実施形態の中継装置１０２は、第１の実施形態の構成例と同様に、第１のＩＥＥＥ１３９４インタフェース（Ｉ／Ｆ）１１０１、第２のＩＥＥＥ１３９４インタフェース（Ｉ／Ｆ）１１０８、第１のＡＶ／Ｃプロトコル処理部１１０２、第２のＡＶ／Ｃプロトコル処理部１１０９、第１のコピープロテクション処理部１１０３、第２のコピープロテクション処理部１１１０、第１のＩＳＯ信号送受信部１１０４、第２のＩＳＯ信号送受信部１１０７、ブリッジテーブル部１１０５、ブリッジ接続処理部１１０６を有する。

【０１００】第１の実施形態との相違点は、各コピープロテクション処理部１１０３，１１１０内にそれぞれ機器証明（Ｃｃｅｒｔ，Ｄｃｅｒｔ）を持っている点（もちろんそれに加えて処理アルゴリズムが相違する点）である。

【０１０１】図９に、本実施形態におけるシーケンス例を示す。

【０１０２】また、図１０に、本実施形態におけるブリッジテーブルの構成例を示す。

【０１０３】シーケンスの初期において、送信装置１０１と受信装置１０３との間、送信装置１０１と中継装置１０２との間、および中継装置１０２と受信装置１０３との間で、ＡＶ／Ｃコマンド（Ｓ１２０１）、ブリッジ接続コマンド（Ｓ１２０２，Ｓ１２０３）、暗号化ＡＶデータ（Ｓ１２０４，Ｓ１２０５）がやり取りされる点は、第１の実施形態と同様である。また、第１の実施形態と同様のタイミングで、ブリッジテーブルが図１０（ａ）、図１０（ｂ）というように登録される。その他のＳ１２０１からＳ１２０５までの手順については説明を省略する。

【０１０４】なお、この時点ではまだ認証要求も認証・鍵交換も行われていない。また、受信装置１０３はまだ暗号鍵Ｋを得ていない。

【０１０５】第１の実施形態と同様に、Ｓ１２０５におけるＡＶストリームを受信した受信装置１０３は、受信したデータが暗号化されていることを認識し、この暗号化データの送信者との間での認証・鍵交換の必要性を認識し、この暗号化データの送信者を突き止めるための手順を行う。このため、認証問い合わせパケットを中継装置に対して送信する（Ｓ１２０６）。実際には、この認証問い合わせパケットは、非同期ストリームにて送られるパケットでもよいが、暗号化ＡＶデータの送信ノードＩＤの値を見て、暗号化ＡＶデータを同期チャネル＃ｙにて送信しているのが中継装置１０２であることがわかるため、中継装置１０２宛の非同期パケットでもよい。この認証問い合わせパケットは、第２のＩＥＥＥ１３９４バス（１０５）上の同期チャネル＃ｙに対してデータを送信しているのが誰なのかを確認するためのパケットである。このパケットには、この暗号化ＡＶデータを受信しているのが、受信装置１０３であることを示すために、同期チャネル番号＃ｙの他に、受信装置１０３のノードＩＤ（Ｂ，ｄ）と、受信しているプラグであるｉＰＣＲ［０］の値等も入っている。

【０１０６】この認証問い合わせパケットを受信した中継装置１０２は、ブリッジテーブルの認証先の欄に、「同期チャネル＃ｙを受信しているのは（Ｂ，ｄ）のｉＰＣＲ［０］である」旨を登録する。さらに、この同期チャネルを送信しているのが第１のＩＥＥＥ１３９４バス上（１０４）の（Ａ，ａ）であることをブリッジテー

ブルを参照することにより確認し、（Ａ，ａ）に対して認証問い合わせを行うことを認識する。このとき、第1の実施形態のように、中継装置１０２がこの認証問い合わせをフォワードするのではなく、本実施形態では、あくまで認証問い合わせを行うのは中継装置１０２であるとして、認証問い合わせを発行する。その際は、同期チャネル番号は、ブリッジテーブルを参照して、第１のＩＥＥＥ１３９４バス（１０４）上の同期チャネルに相当する＃ｘとしておくのはもちろん、ＡＶデータを受信している架空のｉＰＣＲを含め、認証問い合わせの送信元は中継装置１０２の架空のｉＰＣＲであるとして、認証問い合わせを送信する（Ｓ１２０７）。また、ブリッジテーブルに、この架空のＰＣＲの値を登録する。なお、架空のＰＣＲの番号は予め定められた架空のＰＣＲ用の番号の範囲から選択され、架空でない実在のＰＣＲの番号は予め定められた実在のＰＣＲ用の番号の範囲から選択されるものとし、ここでは上記の架空のｉＰＣＲの番号は一例としてｉＰＣＲ［１００］であるものとする。このときのブリッジテーブルの登録内容が図１０（ｃ）である。

【０１０７】この認証問い合わせパケットを受信した送信装置１０１は、同期チャネル＃ｘに対して送信しているのはノードＩＤが（Ａ，ａ）、プラグがｏＰＣＲ［０］である旨を認証応答として返答する（Ｓ１２０８）。このとき、認証応答の送信先は、Ｓ１２０７における認証問い合わせの送信者であった中継装置１０２である。

【０１０８】この認証応答を受信した中継装置１０２は、このパケットを参照して、ブリッジテーブルに送信側の認証先（（Ａ，ａ）、ｏＰＣＲ［０］）を登録するとともに、先の受信装置１０３からの認証問い合わせ（Ｓ１２０６）に対する返答として、あたかも自分の仮想のｏＰＣＲ（ｏＰＣＲ［１００］とする）がＡＶデータの送信を行っているものとして、認証応答を返す（Ｓ１２０９）。また、ブリッジテーブルに、この架空のＰＣＲの値を登録する。このときのブリッジテーブルの登録内容が図１０（ｄ）である。

【０１０９】以上の手続きにより、受信装置１０３は、認証・鍵交換を行うべき相手が、中継装置１０２（ノードＩＤが（Ｂ，ａ）、プラグがｏＰＣＲ［１００］）であることを認識する。この時点で、受信装置１０３と中継装置１０２との間および中継装置１０２と送信装置１０１と間でそれぞれ認証・鍵交換の手続きを行うことができるようになる。

【０１１０】続いて、受信装置１０３は認証要求を中継装置１０２に対して、中継装置１０２は認証要求を送信装置１０１に対して、それぞれ送信する（Ｓ１２１０，Ｓ１２１５）。Ｓ１２１１とＳ１２１６についても同様である。このように第１のＩＥＥＥ１３９４バス（１０４）と第２のＩＥＥＥ１３９４バス（１０５）とで認証・鍵交換は独立に行われる。これは、受信装置１０３は（そのｉＰＣＲ［０］に対して）認証すべき相手先が中継装置１０２（のｏＰＣＲ［１００］）であると認識し、送信装置１０１も（そのｏＰＣＲ［０］に対して）認証すべき相手が中継装置１０２（のｉＰＣＲ［１００］）であると認識しているためである。

【０１１１】以降、送信装置１０１と中継装置１０２との間および中継装置１０２と受信装置１０３との間のそれぞれにおいて、認証要求、認証鍵・交換が行われる（Ｓ１２１０～Ｓ１２３１３，Ｓ１２１５～Ｓ１２１８）。

【０１１２】また、Ｓ１２１４とＳ１２１９においては、送信装置１０１から中継装置１０２に送られてきた、交換鍵Ｋｘおよびシードｎｃの値を、中継装置１０２はそのまま受信装置１０３に対してフォワードする。これによって、送信装置１０１と受信装置１０３との間で暗号鍵Ｋを共有することが可能となり、受信装置１０３において暗号化ＡＶストリームの復号が可能となる。そして、これ以降、第１の実施形態と同様に、中継装置１０２を介して、送信装置１０１と受信装置１０３との間で暗号鍵Ｋによる暗号通信を行うことができる。

【０１１３】（第３の実施形態）次に、第３の実施形態について説明する。

【０１１４】図１１に、本発明を適用するネットワークの全体構成の一例を示す。

【０１１５】本実施形態では、第１のＩＥＥＥ１３９４バス（２１０５）と無線ＬＡＮ（２１０７）との間が第１の中継装置２１０２により接続され、無線ＬＡＮ（２１０７）と第２のＩＥＥＥ１３９４バス（２１０６）との間が第２の中継装置２１０３により接続されている場合に、第１のＩＥＥＥ１３９４バス（２１０５）に接続された送信装置２１０１から第２のＩＥＥＥ１３９４バス（２１０６）に接続された受信装置へＡＶデータを転送する場合を例にとって説明する。このとき、これまでの実施形態と同様に、著作権保護のためにこれらのＡＶデータ（一例としてＭＰＥＧ映像データ）には暗号がかけられた上で送信される場合を考える。

【０１１６】以下では、これまでの実施形態と相違する点を中心に説明する。

【０１１７】本実施形態の送信装置２１０１の内部構成例は基本的には第１の実施形態（図２参照）と同様である。受信装置２１０４の内部構成例も基本的には第１の実施形態（図３参照）と同様である。

【０１１８】図１２に、本実施形態の中継装置（もしくはネットワーク中継装置）２１０５，２１０７の内部構成を示す。

【０１１９】本実施形態の中継装置（２１０５，２１０７）は、ＩＥＥＥ１３９４インタフェース２２０１、無線ＬＡＮインタフェース２２１０、第１のＡＶ／Ｃプロトコル処理部２２０２、第２のＡＶ／Ｃプロトコル処理

部２２０６、第１のコピープロテクション処理部２２０３、第２のコピープロテクション処理部２２０５、第１のＩＳＯ信号送受信部２２０７、第２のＩＳＯ信号送受信部２２０９、ＡＶ／Ｃサブユニット代理処理部２２０４、パケットフォーマット変換部２２０８を有する。

【０１２０】各コピープロテクション処理部２２０３，２２０５内にそれぞれ機器証明（Ｃｃｅｒｔ，Ｄｃｅｒｔ）を持つ。

【０１２１】パケットフォーマット変換部２２０８は、チャネル対応テーブルを持つ。図１３に、第１の中継装置２１０２のチャネル対応テーブルの例を示し、図１４に、第２の中継装置２１０３のチャネル対応テーブルの例を示す。

【０１２２】ここでは、第２の中継装置２１０３について主に述べるが、基本的な動作等は第１の中継装置２１０２も、第２の中継装置２１０３も、同様である（構成自体は同様であるが、一方には送信装置２１０１が接続され、他方には受信装置２１０４が接続されるという相違から、送信装置２１０１から受信装置２１０４へのパケット転送について見たときにパケットの入側または出側がＩＥＥＥ１３９４バス側かまたは無線ＬＡＮ側かという点でＩＥＥＥ１３９４バス側と無線ＬＡＮ側との論理的な機能が入れ替わるところと、また受信装置２１０４に対して受信チャネル確認を行うか否かというところなどが、動作として異なってくる）。なお、以下では、本実施形態の中継装置２１０２，２１０３につては、第２の実施形態における中継装置１０２との相違点を中心に説明する。

【０１２３】図１５に、本実施形態における全体のシーケンス例を示す。

【０１２４】なお、鍵交換前に行われる暗号化ＡＶデータ転送までのシーケンスにおいて、送信装置２１０１から受信装置２１０４へ制御コマンドが転送される点、送信装置２１０１から中継装置２１０２・中継装置２１０３を経て受信装置２１０４までの経路が設定される点については、第１、第２の実施形態と基本的には同様もしくは類似であり、図１５においてはそれらの手順の説明を省略している。

【０１２５】ここで、本実施形態の中継装置（２１０２，２１０３）は、一方のネットワーク上のサービスやサブユニットなどの構成認識を自動的に行い、これらのサービスやサブユニット等を、あたかも自分自身（中継装置自身）のサービスあるいはサブユニットであるとして他方のネットワーク上に見せる機能を持ってもよい。本実施形態では、そのような機能を持つものとして説明している。この機能を実現するのが、ＡＶ／Ｃサブユニット代理処理部２２１０である。なお、このような機能の詳細については、例えば電子情報通信学会ＩＮ研究会９８－２１５等に開示されている。

【０１２６】図１１の例においては、第１の中継装置２１０２が、無線ＬＡＮ（２１０７）側に対して、送信装置２１０１の代理サービスを行っているものとする。これによって、無線ＬＡＮ（２１０７）側では、第１の中継装置２１０２内の一構成要素として、送信装置２１０１（のサービスやサブユニット等）が認識される。

【０１２７】また、第２の中継装置２１０３は、第２のＩＥＥＥ１３９４バス（２１０６）側に対して、第１の中継装置２１０２内の一構成要素である「当該第１の中継装置２１０２が提供している送信装置２１０１の代理サービス」の代理サービスを行っているものとする。つまり、第２の中継装置２１０３は、第２のＩＥＥＥ１３９４バス（２１０６）側に対して、送信装置２１０１の代理サービスを行っている。これによって、第２のＩＥＥＥ１３９４バス（２１０６）側では、第１の中継装置２１０２内の一構成要素として、送信装置２１０１（のサービスやサブユニット等）が認識される。

【０１２８】また、中継装置２１０２，２１０３では、代理サービスを提供している先のネットワーク側からの制御コマンドをそのネットワーク側のＡＶ／Ｃプロトコル処理部で受信し、このコマンドが実際にはどのサービス／サブユニットに宛てて送出されたものであるかをＡＶ／Ｃサブユニット代理処理部２２０４内のテーブルを参照するなどして認識し、代理サービスを行っている元のネットワーク側のＡＶ／Ｃプロトコル処理部を通して、その代理サービスを行っているサービス／サブユニット向けのコマンドに変換し、その元のネットワーク側に送出する。

【０１２９】さて、受信装置２１０４は、上記のようにしてあたかも送信装置２１０１が第２の中継装置２１０３の一構成要素であるかのごとく認識し、第２の中継装置２１０３に対して、その実体は送信装置２１０１であるところの一構成要素に対する制御コマンドを送出する。

【０１３０】第２の中継装置２１０３では、この制御コマンドを、ＩＥＥＥ１３９４バス側から受信する。ここで、この制御コマンドは、自装置が代理している無線ＬＡＮ側の第１の中継装置２１０２の一構成要素（すなわち送信装置２１０１の代理サービス）宛であることが認識される。したがって、該制御パケットを自装置から第１の中継装置２１０２宛になるように変換して、無線ＬＡＮ側に送出する。

【０１３１】第１の中継装置２１０２では、この制御コマンドを、無線ＬＡＮ側から受信する。ここで、この制御コマンドは、自装置が代理しているＩＥＥＥ１３９４バス側の送信装置２１０１宛であることが認識される。したがって、該制御パケットを自装置から送信装置２１０１宛になるように変換して、ＩＥＥＥ１３９４バス側に送出する。

【０１３２】この制御コマンドと前後して、送信装置２１０１から受信装置２１０４へとつながるＱＯＳ（通信

品質）を保証するための通信パスの設定が行われる。詳細は省略するが、第1のＩＥＥＥ１３９４バス（２１０５）上では同期チャネル＃ｘが、無線ＬＡＮ（２１０７）上では通信帯域が確保されたチャネル＃ｙが、第2のＩＥＥＥ１３９４バス（２１０６）上では同期チャネル＃ｚがそれぞれ確保されるものとする。

【０１３３】さて、送信装置２１０１と第1の中継装置２１０２をつなぐ同期チャネル＃ｘ、第１の中継装置２１０２と第2の中継装置２１０３をつなぐ同期チャネル＃ｙ、第2の中継装置２１０３と受信装置２１０３をつなぐ同期チャネル＃ｚが確立された後、送信装置２１０１から暗号化されたＡＶストリームが送信され、第１の中継装置２１０２、第2の中継装置２１０３を介して、受信装置２１０４へ転送される（Ｓ２３０１～Ｓ２３０３）。

【０１３４】すなわち、送信装置２１０１から受信装置２１０４に対して転送される（暗号化された）ＡＶデータは、第1のＩＥＥＥ１３９４バス（２１０５）上の同期チャネル＃ｘを通して、第１の中継装置２１０２に到達する。ここで、ＩＳＯ信号送受信部２２０７、パケットフォーマット変換部２２０８、ＩＳＯ信号送受信部２２０９等を通して、無線ＬＡＮ（２１０７）上のチャネル＃ｙに送出される。以下、同様に、第2の中継装置２１０３を経て、第2のＩＥＥＥ１３９４バス（２１０６）上の同期チャネル＃ｚを通して、受信装置２１０４に到達する。ここで、各中継装置において、暗号化されたＡＶデータの復号化処理は特に行われず、暗号化された部分はそのままの形で（タイムスタンプなどの値や、リンクレイヤヘッダ等は書き換えられる可能性がある）転送される。

【０１３５】本実施形態では、各中継装置２１０３内には、これらのチャネル間の関係を記述するためのチャネル対応テーブルが用意されるが、この時点では、第2の中継装置２１０３のチャネル対応テーブルにおいては、各々の同期チャネル番号、送受信の方向、ＡＶデータの送信者（すなわち、図１４の上3行）についての情報が記述されている。つまり、認証先は確定しておらず、第２の中継装置２１０３は、第2のＩＥＥＥ１３９４バス（２１０６）側に送出しているフローが、どのノード向けのデータであるかについては、認識していない。第１の中継装置２１０２のチャネル対応テーブル（図１３）についても同様である。

【０１３６】さて、暗号化されたＡＶデータを受信した受信装置２１０４は、この暗号化されたＡＶデータを復号化するために必要な、暗号鍵に関する情報を入手するために、予め定められている通り、そのＡＶデータの送信ノードに対して認証要求を送信する（Ｓ２３０４）。この例の場合、受信装置２１０４は、同期チャネル＃ｚを通して送られてくるＡＶデータの送信ノードアドレス（ＣＩＰヘッダ内にあるフィールド）を参照して、これが第2の中継装置２１０３から送られてきているものであることを認識し、第2の中継装置２１０３に対して、認証要求を送信する。

【０１３７】ここで、第1の実施形態（ＩＥＥＥ１３９４上での認証・鍵交換は、ＡＶデータフロー毎あるいはＡＶ／Ｃのプラグ毎に行われ、同じノード間では複数の暗号鍵をフロー毎あるいはプラグ毎に使用することが可能であるものとした）とは異なり、第2のＩＥＥＥ１３９４バス（２１０６）においては、同じノード間（本例の場合、第2の中継装置２１０３と受信装置２１０４との間）では１つの暗号鍵しか定義できないものとする（ただし、同じコピー制御情報のフローについて；例えば、Ｎｅｖｅｒ　Ｃｏｐｙのコンテンツについては、異なるプラグで同時に複数のフローがやり取りされていたとしても、用いられる暗号鍵は同一のものである；なお、コピー制御情報は、例えば、「このデータは何回コピー可」、「このデータはコピー不可」等、送られるデータのコピーをどの様に扱うかが記載されている情報である。）。この点は、第1のＩＥＥＥ１３９４バス（２１０５）側についても（送信装置２１０１と第1の中継装置２１０２との間でも）同様とする。これに対し、無線ＬＡＮ（２１０７）は、第1の実施形態と同様に、同じノード間でフロー毎あるいはプラグ毎に異なる暗号鍵を使うことができるものとする。

【０１３８】このように、複数の「同一のノード間でやり取りするフローに同一の暗号鍵しか用いることの出来ない」ネットワーク間を、「同一のノード間でやり取りするフロー毎に異なる暗号鍵を用いることが出来る」ネットワークで接続するのは、以下のような理由がある。すなわち、第1のＩＥＥＥ１３９４バス（２１０５）上に2つ以上の送信装置（例えば、第１の送信装置と第2の送信装置）、第2のＩＥＥＥ１３９４バス（２１０６）上に2つ以上の受信装置（例えば、第１の受信装置と第2の受信装置）が存在し、第１の送信装置と第1の受信装置との間および第2の送信装置と第2の受信装置との間でそれぞれ暗号化されたＡＶデータやり取りがなされるものとする。この場合、両方のＩＥＥＥ１３９４バス間に位置する無線ＬＡＮがもし「異なるフローに異なる暗号鍵を用いることが出来ない」とすると、上記の２つのフローに対して同じ暗号鍵しか用いることが出来ないことになる。しかし、実際にはどの暗号鍵を使うかは個々の送信装置（例えば第１の送信装置と第2の送信装置）がそれぞれ独立に決定することであり、これの例で言えば２つの鍵が同一の値になる保証はない。よって、無線ＬＡＮにおいてフロー毎に鍵が定義できないと、上記２つの暗号化フローを無線ＬＡＮ上に転送することが不可能となる。反対に、無線ＬＡＮ（２１０７）においてフロー毎に鍵が定義できれば、たとえ第1と第2のＩＥＥＥ１３９４バス（２１０５，２１０６）が同一ノード間では単一鍵のサポートしか行っていない場合

においても、無線ＬＡＮ（２１０７）を使った相互接続の環境で、複数の送信装置から出力される複数のフローを同時にやり取りすることが可能となる。

【０１３９】さて、これを実現するためには、第２の中継装置２１０３には工夫が必要である。すなわち、受信装置２１０４から認証要求を受け取ったとしても、その認証要求には、「どのフローに関する認証要求か」についての情報は記載されておらず、最終的な鍵交換において、どのフローのための鍵を送信しなければいけないかの判断がつかないという問題がある。そこで、受信装置２１０４からＳ２３０４の認証要求を受信した第２の中継装置２１０３は、この認証要求がどのチャネル（どのプラグ）が提供している暗号化ＡＶフローに対する認証要求であるかの調査を行うべく、受信装置２１０４に対して、受信チャネル確認パケットを送信する（Ｓ２３０５）。このパケットは、「あなたはどのチャネル／プラグで（暗号化ＡＶデータの）受信を行っているか」について、受信装置２１０４に問い合わせを行うためのパケットである。これに対し、受信装置２１０４は受信チャネル（本実施形態の場合は、＃ｚ）を応答する（Ｓ２３０６）。

【０１４０】この受信チャネル確認パケットの手続き（Ｓ２３０５，Ｓ２３０６）は、受信装置２１０４のプラグに関するレジスタを読み取ることにより、受信装置２１０４がどのチャネルのデータを受信しているかどうかを第２の中継装置２１０３が調査することにより、代用してももちろんよい。

【０１４１】受信装置２１０４が受信している同期チャネル番号（本例では、＃ｚ）を得た第２の中継装置２１０３は、内部のチャネル間の関係を記述したチャネル対応テーブルを参照し、「第２のＩＥＥＥ１３９４側に同期チャネル＃ｚにて送信しているのは、無線ＬＡＮ側ではチャネル＃ｙであり、無線ＬＡＮ側にてチャネル＃ｙに送信しているのは第１の中継装置である」ということを認識する。つまり、第１の中継装置２１０２（のｏＰＣＲ［０］）から受信されているフローが、第２のＩＥＥＥ１３９４バス（２１０６）の同期チャネル＃ｚにフォワードされていることを知る。これを、図１４のチャネル対応テーブル（第２のＩＥＥＥ１３９４側の認証先と受信者の欄）に登録する。

【０１４２】さて、第１の中継装置２１０２と第２の中継装置２１０３との間では、第１の実施形態にて述べたような認証・鍵交換の手続き（認証手続きにおいて、フローやプラグの単位まで指定して、これを行う）がこれと前後して行われる（Ｓ２３１０～Ｓ２３１５）。Ｓ２３１０の際に図１４のチャネル対応テーブルの無線ＬＡＮ側の受信者の欄が登録され、Ｓ２３１１の際に無線ＬＡＮ側の認証先の欄が登録される。また、Ｓ２３１０の際に図１３のチャネル対応テーブルの無線ＬＡＮ側の認証先・受信者の欄が登録され、Ｓ２３１１の際に無線ＬＡＮ側の自分自身のプラグ番号が登録される。

【０１４３】また、送信装置２１０１と第１の中継装置２１０２との間では、これと前後して、ノード間、すなわち第２の中継装置２１０３と受信装置２１０４との間と同様の形（ただし、受信チャネルの確認を行う必要はない）で、認証・鍵交換が行われる（Ｓ２３１６～Ｓ２３１９）。Ｓ２３１６の際に図１３のチャネル対応テーブルのＩＥＥＥ１３９４側の認証先・受信者の欄が登録される。

【０１４４】なお、第２の中継装置２１０３と受信装置２１０４との間でも、残りの認証要求と、認証・鍵交換手続きが行われる（Ｓ２３０７～Ｓ２３０９）。

【０１４５】第１の中継装置２１０２は、第２の中継装置２１０３と第１の中継装置２１０２との間で行われる認証・鍵交換の手続きが、（第１の中継装置２１０２の出力プラグｏＰＣＲ［０］が指定されているため、第１の中継装置２１０２におけるチャネル間の関係を記述したチャネル対応テーブル（図１３）を参照することにより）、送信装置２１０１と第１の中継装置２１０２との間の認証・鍵交換と結びつければよいことを認識することができる。そのため、第１の中継装置２１０２は、送信装置２１０１と第１の中継装置２１０２との間で行われる認証・鍵交換の結果、第１の中継装置２１０２に通知される交換鍵Ｋｘとシードｎｃの値を、第２の中継装置２１０３に対して（出力プラグが第１の中継装置２１０２のｏＰＣＲ［０］、入力プラグが第２の中継装置２１０３のｉＰＣＲ［０］であることを指定して）フォワードすることができる（Ｓ２３２０，Ｓ２３２１）。

【０１４６】同様に、第２の中継装置２１０３は、第１の中継装置２１０２と第２の中継装置２１０３との間で行われる認証・鍵交換の結果、第２の中継装置２１０３に通知される交換鍵Ｋｘとシードｎｃの値を、第２の中継装置２１０３におけるチャネル間の関係を記述したチャネル対応テーブル（図１４）を参照することにより、これらの鍵が第２のＩＥＥＥ１３９４バス（２１０６）側の同期チャネル＃ｚに関するものであり、その受信先が受信装置２１０４であることを認識することができるため、受信装置２１０４に対して（出力プラグが第２の中継装置２１０３のｏＰＣＲ［０］、入力プラグが受信装置２１０４のｉＰＣＲ［０］であることを指定して）フォワードすることができる（Ｓ２３２１，Ｓ２３２２）。

【０１４７】なお、図１４のチャネル対応テーブルは、第２のＩＥＥＥ１３９４バス（２１０６）上の同一の同期チャネル（例えば、＃ｚ）について複数の受信者が存在する場合は、その受信装置の数だけ用意する。これにより、各々の受信装置に対して、正確に鍵の値などを通知することが可能となる。

【０１４８】上記の点は、第１のＩＥＥＥ１３９４バス（２１０５）上の同一の同期チャネル（例えば、＃ｘ）

について複数の送信者が存在する場合における図１３のチャネル対応テーブルについても同様である。

【０１４９】このようにして、交換鍵Ｋｘおよびシードナンバーの値を受け取った受信装置２１０４は、第１の実施形態と同様に、暗号鍵の値を計算することができ、暗号化されたＡＶデータの復号化を行うことができる。

【０１５０】第１および第２の中継装置（２１０２，２１０３）は、暗号化されたＡＶデータを復号化することなく次段のチャネルにフォワードすることができるため、中継装置を通過する毎に暗号の復号化および再暗号化を行う必要がなくなり、大幅な処理コストの低減を図ることができるようになる。

【０１５１】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０１５２】また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０１５３】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１５４】

【発明の効果】本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図１】本発明の第１、第２の実施形態に係るネットワークの全体構成の一例を示す図

【図２】本発明の第１、第２、第３の実施形態に係る送信装置の内部構造の一例を示す図

【図３】本発明の第１、第２、第３の実施形態に係る受信装置の内部構造の一例を示す図

【図４】本発明の第１の実施形態に係る中継装置の内部構造の一例を示す図

【図５】本発明の第１の実施形態に係るブリッジテーブルの一例を示す図

【図６】本発明の第１の実施形態に係る全体のシーケンスの一例を示す図

【図７】本発明の第１の実施形態に係る中継装置の動作手順の一例を示すフローチャート

【図８】本発明の第２の実施形態に係る中継装置の内部構造の一例を示す図

【図９】本発明の第２の実施形態に係る全体のシーケンスの一例を示す図

【図１０】本発明の第２の実施形態に係るブリッジテーブルの一例を示す図

【図１１】本発明の第３の実施形態に係るネットワークの全体構成の一例を示す図

【図１２】本発明の第３の実施形態に係る第１、第２の中継装置の内部構造の一例を示す図

【図１３】本発明の第３の実施形態に係る第１の中継装置内のチャネル対応テーブルの一例を示す図

【図１４】本発明の第３の実施形態に係る第２の中継装置内のチャネル対応テーブルの一例を示す図

【図１５】本発明の第３の実施形態に係る全体のシーケンスの一例を示す図

【符号の説明】

１０１，２１０１…送信装置

１０２，２１０２，２１０３…中継装置

１０３，２１０４…受信装置

１０４，１０５，２１０５，２１０６…ＩＥＥＥ１３９４バス

２０１，３０１，４０１，４０８，１１０１，１１０８，２２０１…ＩＥＥＥ１３９４インタフェース

２０２，３０２，４０２，４０９，１１０２，１１０９，２２０２，２２０６…ＡＶ／Ｃプロトコル処理部

２０３，３０３，４０３，４１０，１１０３，１１１０，２２０３，２２０５…コピープロテクション処理部

２０４，３０４，４０４，４０７，１１０４，１１０７，２２０７，２２０９…ＩＳＯ信号送受信部

２０５…暗号化部

２０６，３０６…ＭＰＥＧストレージ部

３０５…暗号復号化部

３０７…ディスプレイ部

４０５，１１０５…ブリッジテーブル部

４０６，１１０６…ブリッジ接続処理部

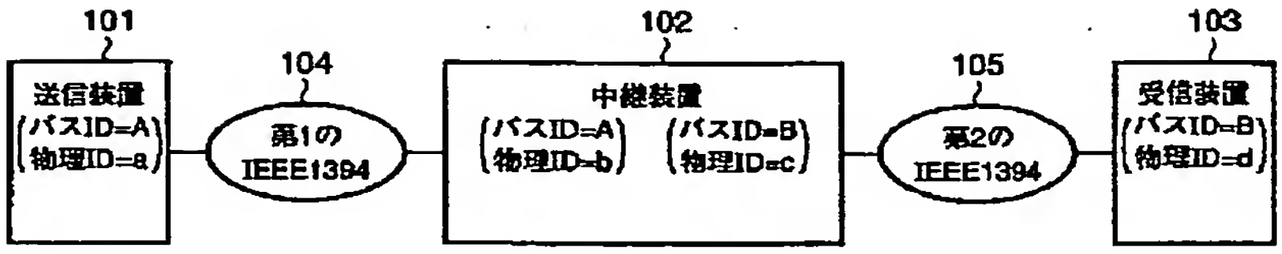
２１０７…無線ＬＡＮ

２２０４…ＡＶ／Ｃサブユニット代理処理部

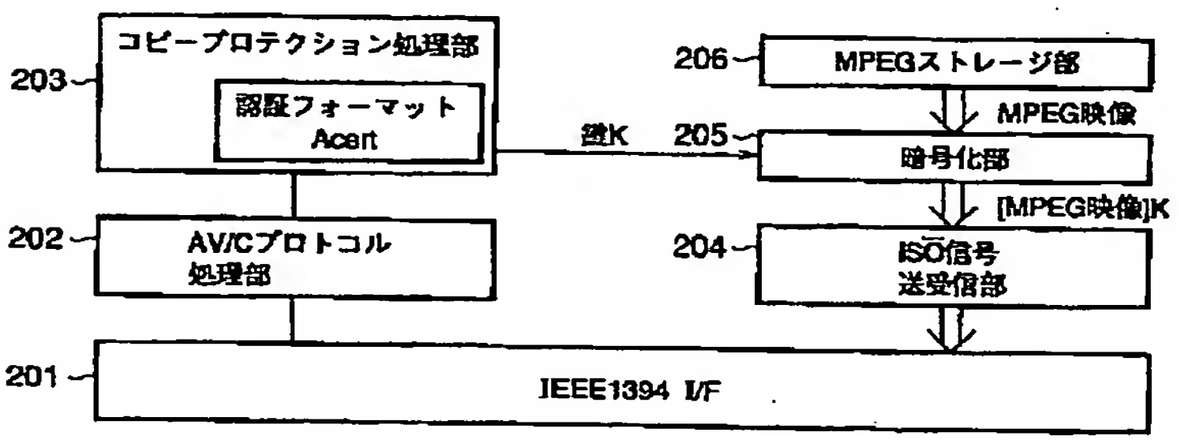
２２０８…パケットフォーマット変換部

２２１０…無線ＬＡＮインタフェース

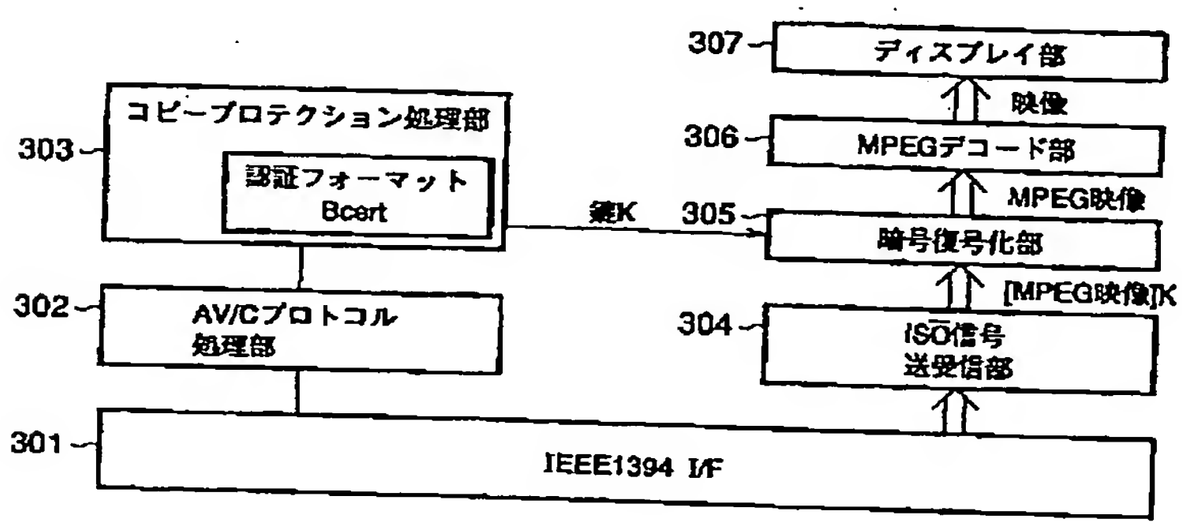
【図1】


101
送信装置
(バスID=A)
(物理ID=a)
104
第1の
IEEE1394
102
中継装置
(バスID=A)
(物理ID=b)
(バスID=B)
(物理ID=c)
105
第2の
IEEE1394
103
受信装置
(バスID=B)
(物理ID=d)

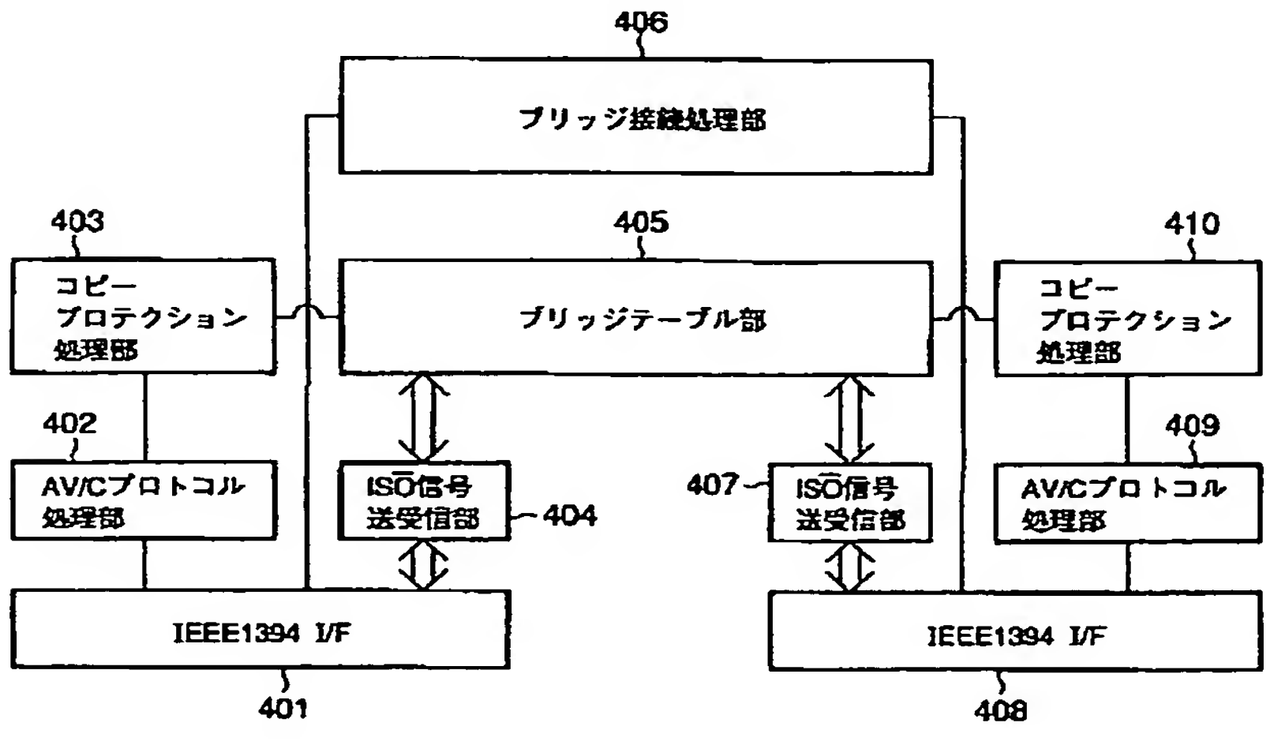
【図2】


203
コピープロテクション処理部
認証フォーマット
Acert
鍵K
205
206
MPEGストレージ部
MPEG映像
暗号化部
[MPEG映像]K
204
ISO信号
送受信部
202
AV/Cプロトコル
処理部
201
IEEE1394 I/F

【図3】


307
ディスプレイ部
映像
306
MPEGデコード部
MPEG映像
303
コピープロテクション処理部
認証フォーマット
Bcert
鍵K
305
暗号復号化部
[MPEG映像]K
302
AV/Cプロトコル
処理部
304
ISO信号
送受信部
301
IEEE1394 I/F

【図4】


406
ブリッジ接続処理部
403
コピー
プロテクション
処理部
405
ブリッジテーブル部
410
コピー
プロテクション
処理部
402
AV/Cプロトコル
処理部
ISO信号
送受信部
404
407
ISO信号
送受信部
409
AV/Cプロトコル
処理部
IEEE1394 I/F
401
IEEE1394 I/F
408

【図5】

(a)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
	送信者	
	認証先	

(b)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
(A,a)	送信者	自分自身
	認証先	

(c)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
(A,a)	送信者	自分自身
	認証先	(B,d),iPCR[0]

(d)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
(A,a)	送信者	自分自身
(A,a),oPCR[0]	認証先	(B,d),iPCR[0]

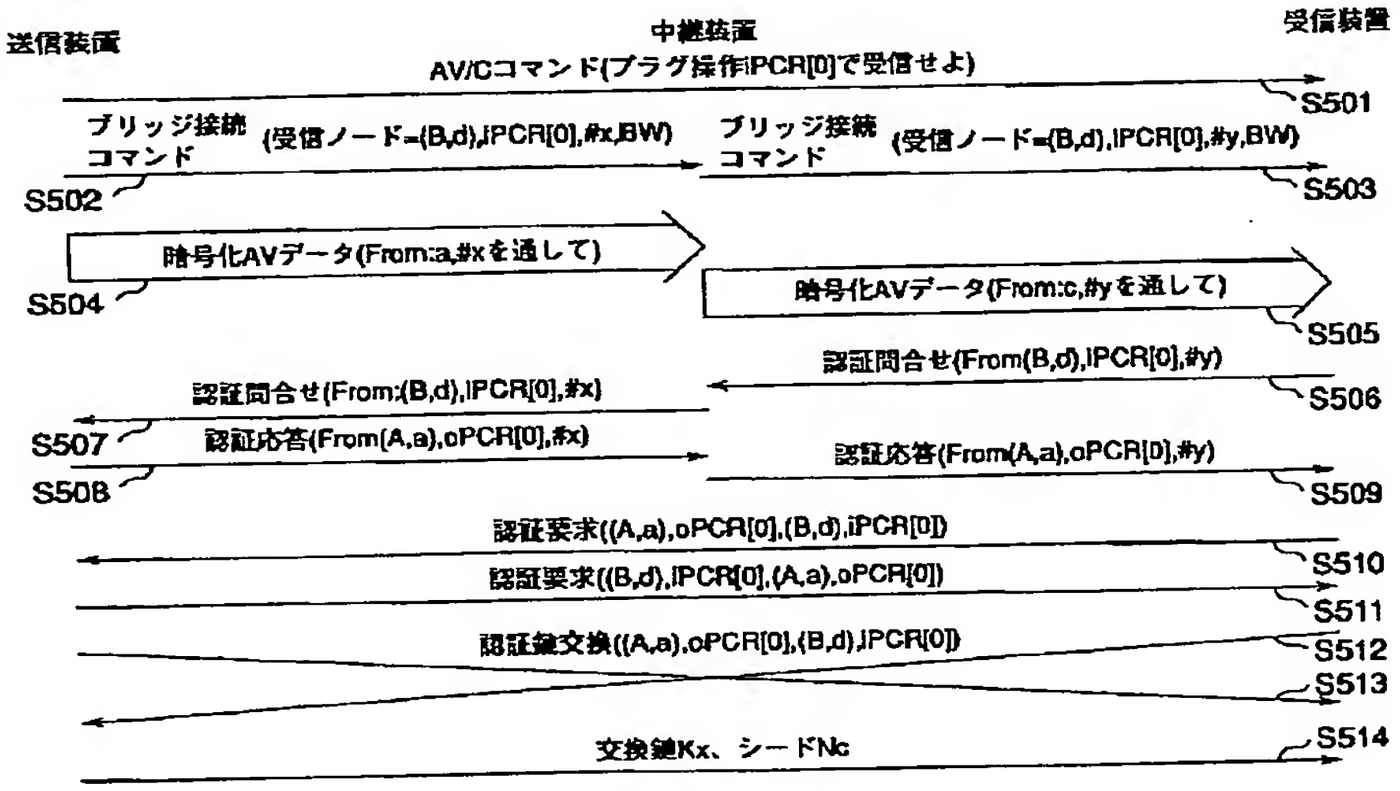
【図13】

第1のIEEE1394側		無線LAN側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
送信装置	送信者	自分自身の oPCR[0]
送信装置	認証先	第2の中継装置の iPCR[0]
自分自身	受信者	第2の中継装置の iPCR[0]

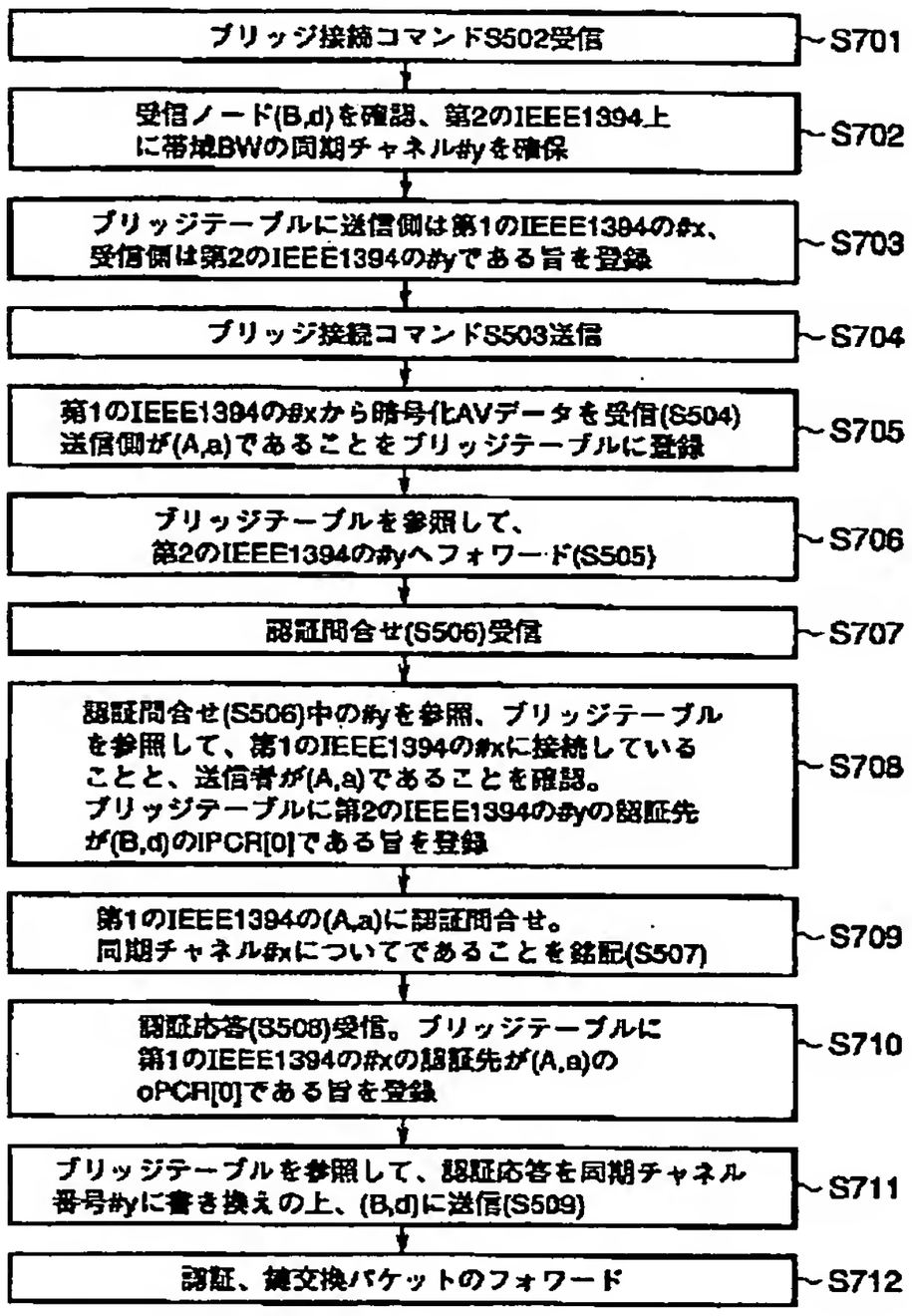
【図14】

無線LAN側		第1のIEEE1394側
#y	同期チャネル番号	#z
送信側	送受信の方向	受信側
第1の中継装置	送信者	自分自身
第1の中継装置の oPCR[0]	認証先	受信装置
自分自身の iPCR[0]	受信者	受信装置

【図6】



【図7】



【図10】

(a)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
	送信者	
	自分自身の仮想的なプラグ	
	認証先	

(b)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
(A,a)	送信者	自分自身
	自分自身の仮想的なプラグ	
	認証先	

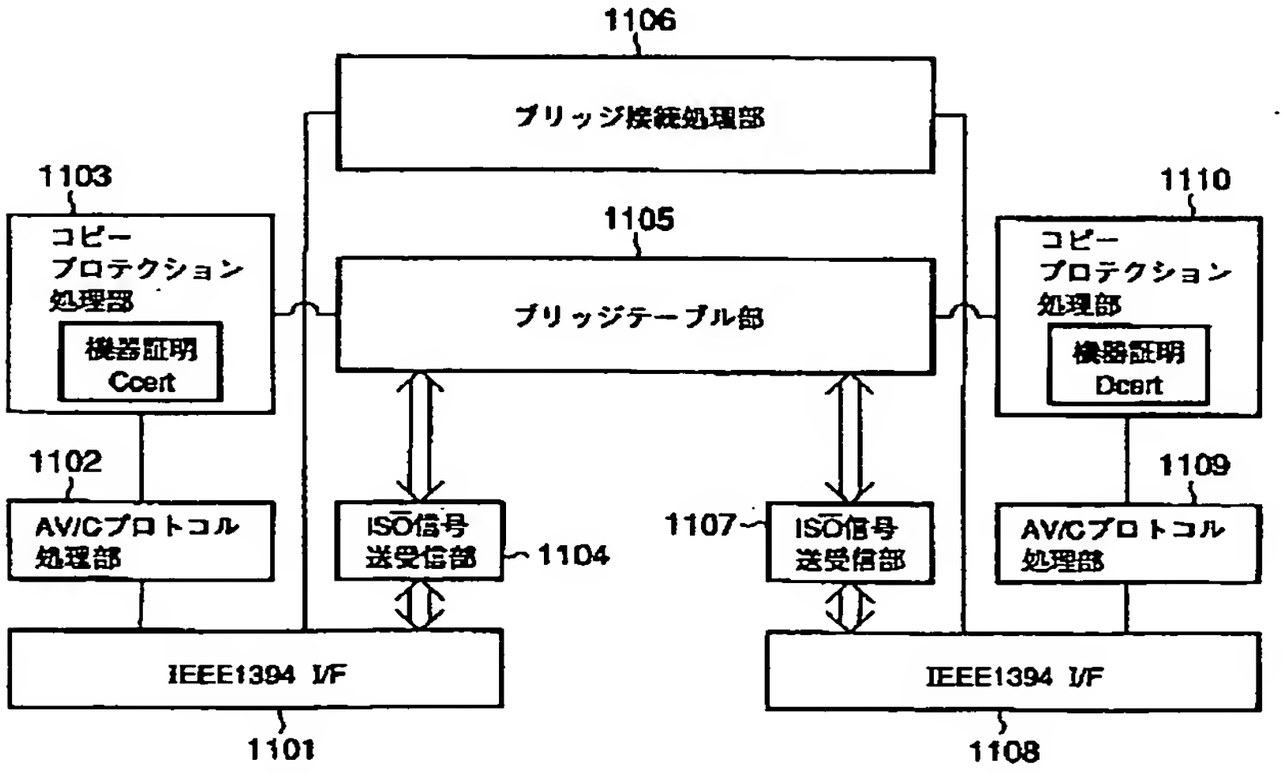
(c)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
(A,a)	送信者	自分自身
iPCR[100]	自分自身の仮想的なプラグ	
	認証先	(B,d),iPCR[0]

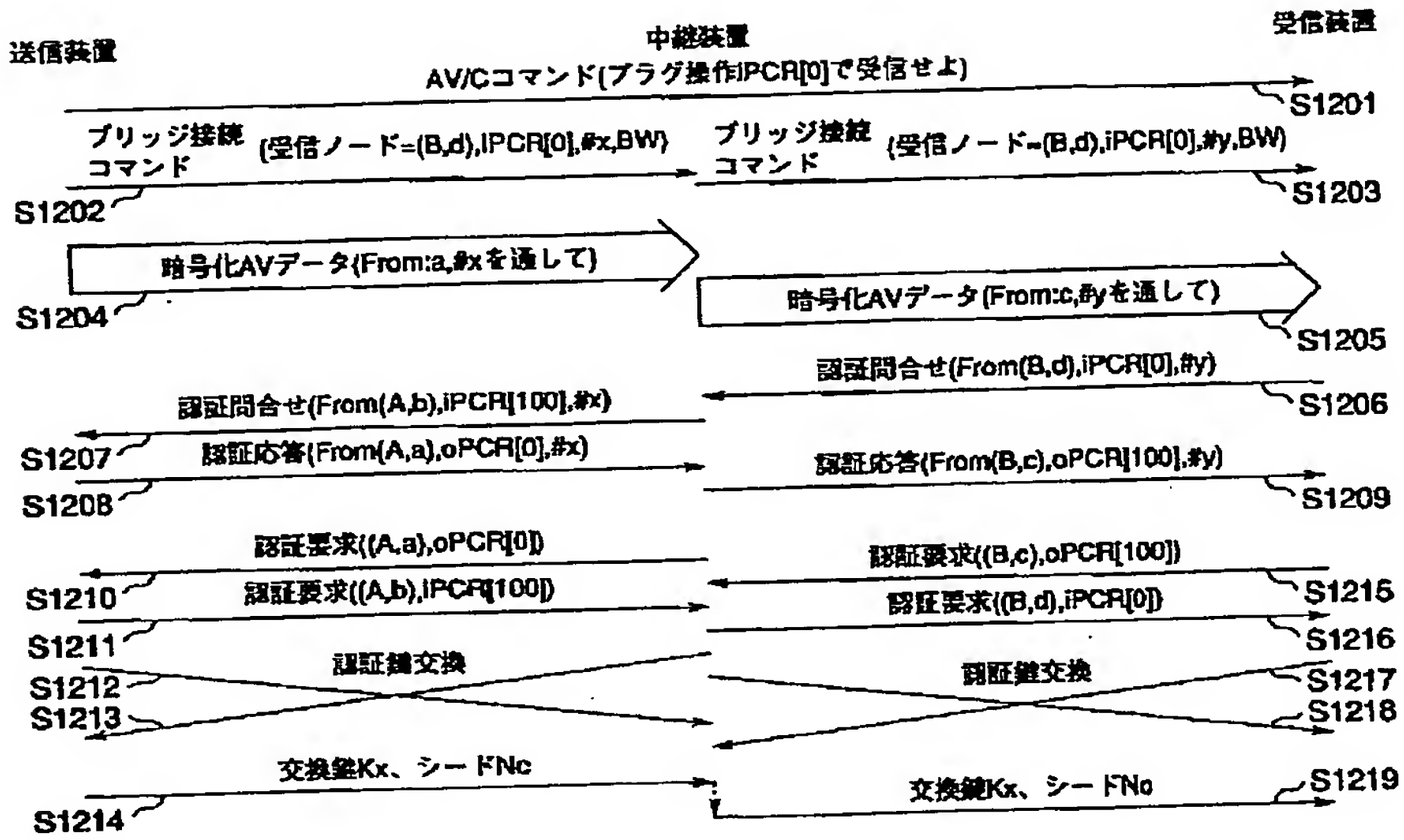
(d)

第1のIEEE1394側		第2のIEEE1394側
#x	同期チャネル番号	#y
送信側	送受信の方向	受信側
(A,a)	送信者	自分自身
iPCR[100]	自分自身の仮想的なプラグ	oPCR[100]
(A,a),oPCR[0]	認証先	(B,d),iPCR[0]

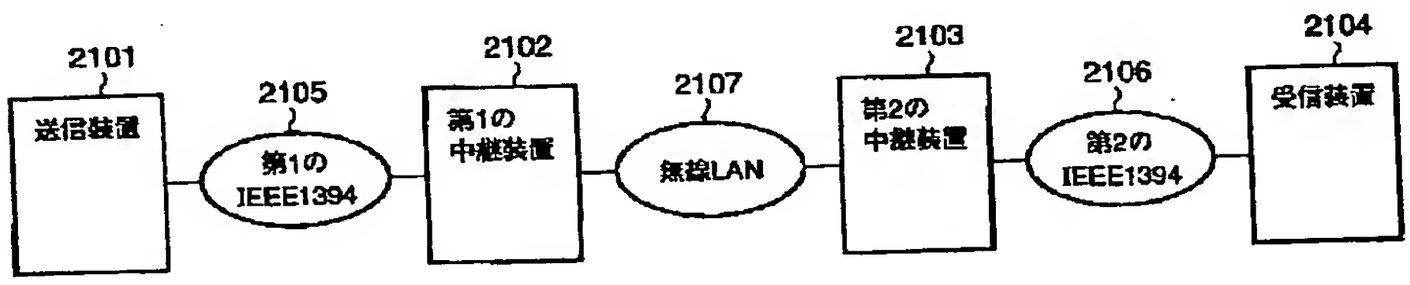
【図8】



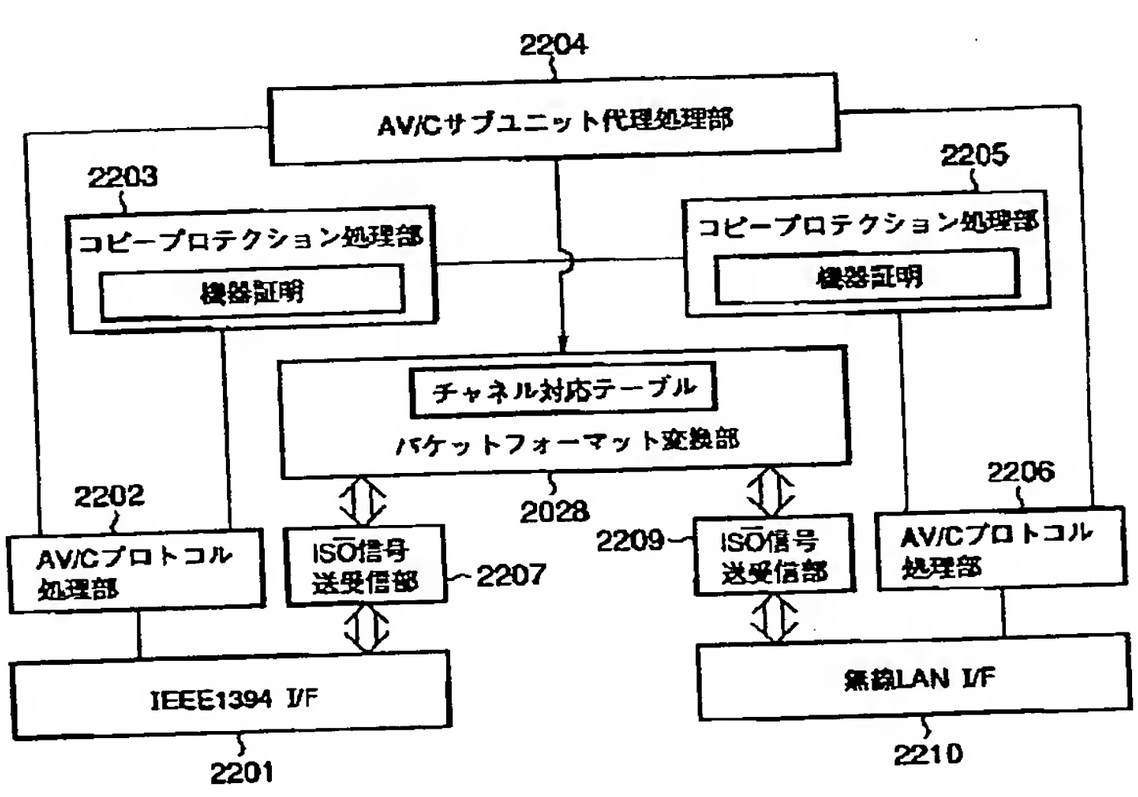
【図9】


送信装置
中継装置
受信装置
AV/Cコマンド(プラグ操作iPCR[0]で受信せよ)
S1201
ブリッジ接続コマンド
(受信ノード=(B,d),iPCR[0],#x,BW)
S1202
ブリッジ接続コマンド
(受信ノード=(B,d),iPCR[0],#y,BW)
S1203
暗号化AVデータ(From:a,#xを通して)
S1204
暗号化AVデータ(From:c,#yを通して)
S1205
認証問合せ(From(B,d),iPCR[0],#y)
S1206
認証問合せ(From(A,b),iPCR[100],#x)
S1207
認証応答(From(A,a),oPCR[0],#x)
S1208
認証応答(From(B,c),oPCR[100],#y)
S1209
認証要求((A,a),oPCR[0])
S1210
認証要求((B,c),oPCR[100])
S1215
認証要求((A,b),iPCR[100])
S1211
認証要求((B,d),iPCR[0])
S1216
認証鍵交換
S1212
S1213
認証鍵交換
S1217
S1218
交換鍵Kx、シードNc
S1214
交換鍵Kx、シードNo
S1219

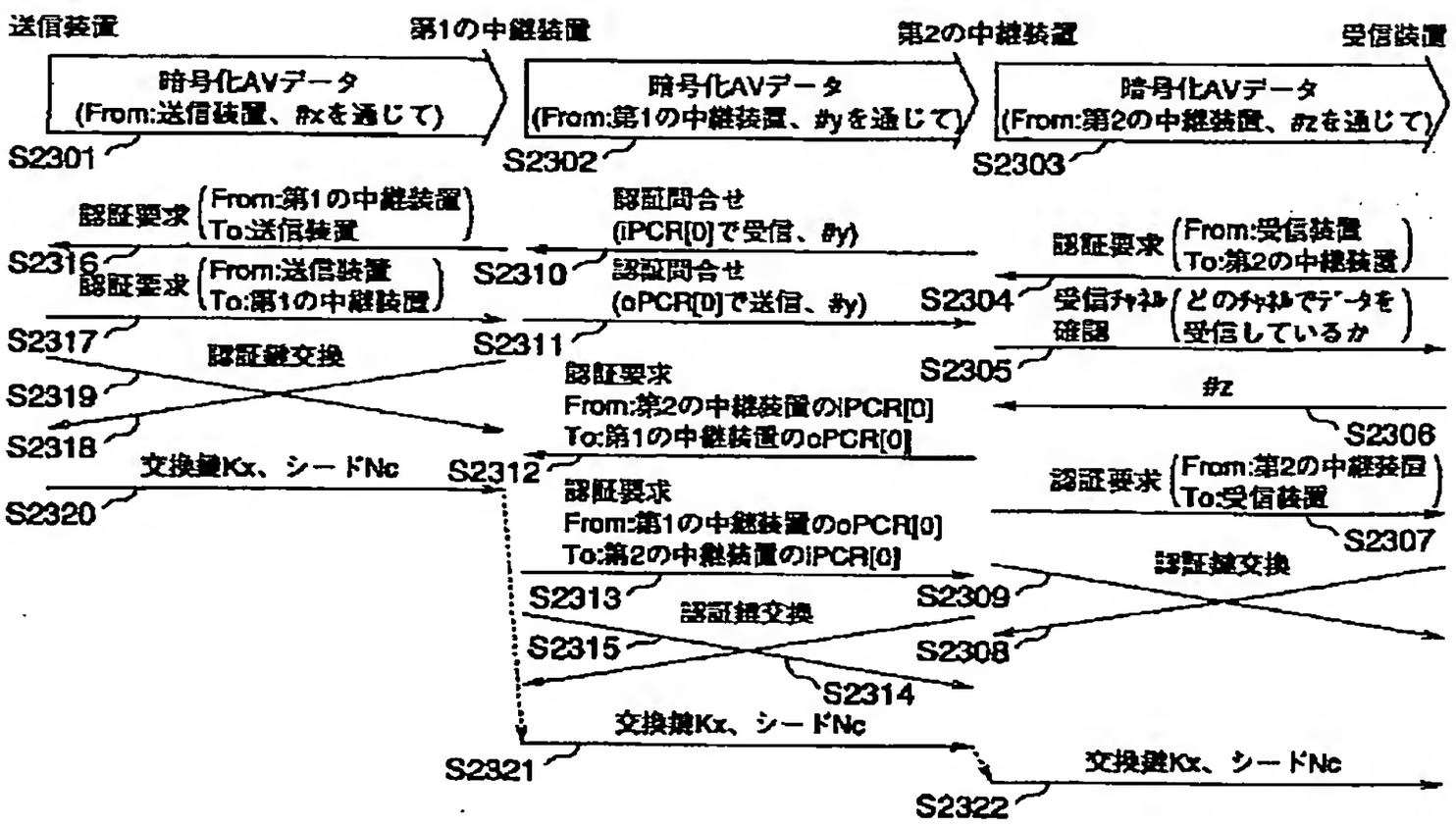
【図11】


2101
送信装置
2105
第1の IEEE1394
2102
第1の中継装置
2107
無線LAN
2103
第2の中継装置
2106
第2の IEEE1394
2104
受信装置

【図12】


2204
AV/Cサブユニット代理処理部
2203
コピープロテクション処理部
機器証明
2205
コピープロテクション処理部
機器証明
チャネル対応テーブル
パケットフォーマット変換部
2028
2202
AV/Cプロトコル処理部
ISO信号送受信部
2207
2209
ISO信号送受信部
2206
AV/Cプロトコル処理部
IEEE1394 I/F
2201
無線LAN I/F
2210

【図15】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04L 12/66 12/56		H04L 11/20	102A 9A001

(72)発明者 橋本 幹生
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

Fターム(参考) 5B077 AA21 MM02 NN02
5J104 AA07 KA02 NA02 NA05 PA07
5K030 GA15 HA08 HB21 HD01 HD06 JA11 JL01 KA19 LD20
5K032 AA08 BA16 CD01 DA06 DA21 DB15 DB26
5K033 AA08 BA15 CC01 DA05 DB10 DB18
9A001 BB04 CC05 CC07 DD10 EE03 JZ19 LL03